



Operation/Reference Guide

# NXA-WAP250G

802.11 b/g Wireless Access Point  
for Modero Touch Panels



# AMX Limited Warranty and Disclaimer

AMX warrants its products to be free of defects in material and workmanship under normal use for three (3) years from the date of purchase from AMX, with the following exceptions:

- Electroluminescent and LCD Control Panels are warranted for three (3) years, except for the display and touch overlay components that are warranted for a period of one (1) year.
- Disk drive mechanisms, pan/tilt heads, power supplies, and MX Series products are warranted for a period of one (1) year.
- AMX Lighting products are guaranteed to switch on and off any load that is properly connected to our lighting products, as long as the AMX Lighting products are under warranty. AMX does guarantee the control of dimmable loads that are properly connected to our lighting products. The dimming performance or quality cannot be guaranteed due to the random combinations of dimmers, lamps and ballasts or transformers.
- Unless otherwise specified, OEM and custom products are warranted for a period of one (1) year.
- AMX Software is warranted for a period of ninety (90) days.
- Batteries and incandescent lamps are not covered under the warranty.

This warranty extends only to products purchased directly from AMX or an Authorized AMX Dealer.

All products returned to AMX require a Return Material Authorization (RMA) number. The RMA number is obtained from the AMX RMA Department. The RMA number must be clearly marked on the outside of each box. The RMA is valid for a 30-day period. After the 30-day period the RMA will be cancelled. Any shipments received not consistent with the RMA, or after the RMA is cancelled, will be refused. AMX is not responsible for products returned without a valid RMA number.

AMX is not liable for any damages caused by its products or for the failure of its products to perform. This includes any lost profits, lost savings, incidental damages, or consequential damages. AMX is not liable for any claim made by a third party or by an AMX Dealer for a third party.

This limitation of liability applies whether damages are sought, or a claim is made, under this warranty or as a tort claim (including negligence and strict product liability), a contract claim, or any other claim. This limitation of liability cannot be waived or amended by any person. This limitation of liability will be effective even if AMX or an authorized representative of AMX has been advised of the possibility of any such damages. This limitation of liability, however, will not apply to claims for personal injury.

Some states do not allow a limitation of how long an implied warranty last. Some states do not allow the limitation or exclusion of incidental or consequential damages for consumer products. In such states, the limitation or exclusion of the Limited Warranty may not apply. This Limited Warranty gives the owner specific legal rights. The owner may also have other rights that vary from state to state. The owner is advised to consult applicable state laws for full determination of rights.

**EXCEPT AS EXPRESSLY SET FORTH IN THIS WARRANTY, AMX MAKES NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. AMX EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED TO THE TERMS OF THIS LIMITED WARRANTY.**

# Table of Contents

<b>Compliances .....</b>	<b>1</b>
Federal Communication Commission Interference Statement .....	1
IMPORTANT NOTE: FCC Radiation Exposure Statement .....	1
EC Conformance Declaration .....	2
<b>NXA-WAP250G .....</b>	<b>3</b>
Overview .....	3
Specifications .....	3
Power Connector .....	4
Ethernet Port .....	4
Reset Button .....	4
<b>Installation .....</b>	<b>5</b>
Overview .....	5
Access Point Configuration .....	6
Twisted-Pair Cable Assignments .....	6
Straight-Through Wiring .....	6
Hardware Description .....	7
Reset Button Overview .....	7
LED Indicators .....	7
Diagnosing Access Point Indicators .....	8
<b>Initial Configuration .....</b>	<b>9</b>
Selecting an Operation Mode .....	9
Access Point Mode .....	9
Access Point Mode - Roaming .....	10
Access Point Mode - Repeater and Bridge Mode .....	11
Logging into the Web Interface .....	12
Using the Setup Wizard .....	13
Step 1: Operation Mode Setting .....	13
Step 2: Network Setting .....	14
DHCP Server/NAT Setting .....	16
Step 3: Wireless VAP #1 Setting .....	16
Step 4: Wireless VAP #2 Setting .....	18
Finish and Reboot .....	19
<b>System Configuration .....</b>	<b>21</b>
Information .....	22
Information - System .....	23
Information - Client .....	24

Information - Network.....	25
Information - Event Log.....	25
<b>System Setting.....</b>	<b>26</b>
System Setting - Administration .....	26
System Setting - VLAN Status / Operation Mode .....	27
System Setting - VAP Management.....	28
System Settings - Reset System .....	28
<b>Wireless VAP Settings.....</b>	<b>29</b>
Wireless VAP Settings - Basic Setting.....	29
Wireless VAP Settings - Channel Setting.....	30
Wireless VAP Settings - WEP Setting .....	31
Wireless VAP Settings - WPA / WPA2 Setting.....	33
<b>Network Settings.....</b>	<b>34</b>
Network Settings - DHCP Client Setting .....	34
Network Settings - DHCP Server/NAT Setting.....	35
Network Settings - PPPoE Setting .....	36
Network Settings - Radius Server Setting .....	37
<b>Time and Log .....</b>	<b>38</b>
<b>Updating Firmware .....</b>	<b>39</b>
Upgrade via the Web Page .....	39
Upgrade via a Remote Server .....	40
<b>Appendix A: Troubleshooting .....</b>	<b>43</b>
Overview .....	43
<b>If Your WAP250G Is Stuck on the Emergent Recovery Screen.....</b>	<b>43</b>
Step 1: Website for free TFTP Server.....	43
Step 2: Choose Download site and Install TFTP Server .....	43
Step 3: Copy Firmware file .....	44
Step 4: Ethernet Connectivity .....	44
Step 5: Launch TFTP Server.....	44
Step 6: Change TFTP Server Settings.....	44
Step 7: Re-Connect to WAP 250G.....	45

# Compliances

## Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

**FCC Caution:** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

## IMPORTANT NOTE: FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

## EC Conformance Declaration

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

- EN 60950-1 (IEC 60950-1) - Product Safety
- EN 300 328 - Technical requirements for 2.4 GHz radio equipment
- EN 301 489-1, EN 301 489-17 - EMC requirements for radio equipment

This device is intended for use in the following European Community countries:

- |               |                  |               |
|---------------|------------------|---------------|
| • Austria     | • Belgium        | • Denmark     |
| • Finland     | • France         | • Germany     |
| • Italy       | • Luxembourg     | • Netherlands |
| • Norway      | • Spain          | • Sweden      |
| • Switzerland | • United Kingdom | • Portugal    |
| • Greece      | • Ireland        | • Iceland     |

Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below:

- In Italy the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
- In Belgium outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
- In France outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.

# NXA-WAP250G

## Overview

AMX's new NXA-WAP250G 802.11b/g Wireless Access Point (**FG2255-50**) provides both high performance and increased security to support all of AMX's G4 Modero wireless touch panels. The NXA-WAP250G (FIG. 1) provides convenient WLAN access for office/home computers with connection speeds of up to 54Mbps. This Wi-Fi certified WAP incorporates wireless encryption standards such as enterprise-grade WPA2, WPA, 802.1x, MAC Address filtering, and 64-bit/128-bit WEP encryption.



**FIG. 1** NXA-WAP250G Wireless Access Point

## Specifications

NXA-WAP250G (FG2255-50) Specifications	
<b>Maximum Channels</b>	<ul style="list-style-type: none"> <li>FCC/IC: 1-11</li> <li>ETSI: 1-13</li> <li>MKK: 1-13</li> </ul>
<b>Maximum Clients</b>	32 per VAP interface
<b>Data Rate</b>	<ul style="list-style-type: none"> <li>802.11g: 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps per channel</li> <li>802.11b: 1, 2, 5.5, 11 Mbps per channel</li> </ul>
<b>Modulation Type</b>	<ul style="list-style-type: none"> <li>802.11g: CCK, BPSK, QPSK, OFDM</li> <li>802.11b: CCK, BPSK, QPSK</li> </ul>
<b>Network Configuration</b>	Infrastructure
<b>Operating Frequency</b>	<ul style="list-style-type: none"> <li>2.4 ~ 2.4835 GHz (US, Canada, ETSI)</li> <li>2.4 ~ 2.483 GHz (Japan)</li> </ul>
<b>Wireless Output Power</b>	<ul style="list-style-type: none"> <li>802.11b: 18 dBm (typical)</li> <li>802.11g: 17 dBm @ 6 Mbps, 14dBm @ 54 Mbps</li> </ul>
<b>Wireless Receive Sensitivity</b>	<ul style="list-style-type: none"> <li>802.11b: -90 dBm @ 1 Mbps, -84 dBm @ 11 Mbps</li> <li>802.11g: -86 dBm @ 6 Mbps, -68 dBm @ 54 Mbps</li> </ul>
<b>AC Power Adapter</b>	<ul style="list-style-type: none"> <li>Input: 100-240 VAC, 50-60 Hz</li> <li>Output: 5 VDC, 2 A</li> </ul>
<b>Unit Power Supply</b>	<ul style="list-style-type: none"> <li>DC Input: 5 VDC, 2 A maximum</li> <li>Power Consumption: 6.5 W maximum</li> </ul>
<b>LED Indicators</b>	<ul style="list-style-type: none"> <li>POWER (Power),</li> <li>LAN (Ethernet Link/Activity),</li> <li>WLAN (Wireless Link/Activity)</li> </ul>

NXA-WAP250G Specifications (Cont.)	
<b>Network Management</b>	Web-browser
<b>Temperature</b>	<ul style="list-style-type: none"> <li>• Operating: 0 to 50 °C (32 to 122 °F)</li> <li>• Storage: -20 to 70 °C (32 to 158 °F)</li> </ul>
<b>Humidity</b>	15% to 95% (non-condensing)
<b>Compliances</b>	<ul style="list-style-type: none"> <li>• FCC Part 15B Class B</li> <li>• EN 55022 Class B</li> <li>• EN 55024</li> <li>• EN61000-3-2</li> <li>• EN61000-3-3</li> </ul>
<b>Standards</b>	<ul style="list-style-type: none"> <li>• IEEE 802.3-2005 10BASE-T, 100BASE-TX</li> <li>• IEEE 802.11b, g</li> <li>• Wi-Fi 11b/g, WPA, WPA2, WMM</li> </ul>
<b>Radio Signal Certification</b>	<ul style="list-style-type: none"> <li>• FCC Part 15C 15.247, 15.207 (2.4 GHz)</li> <li>• EN 300-328</li> <li>• EN 301 489-1</li> <li>• EN 301 489-17</li> <li>• ARIB STD-T66</li> <li>• IC RSS-210</li> </ul>
<b>Safety</b>	<ul style="list-style-type: none"> <li>• EN 60950-1</li> <li>• IEC 60950-1 (CB)</li> </ul>
<b>Included Accessories:</b>	<ul style="list-style-type: none"> <li>• AC power adapter set (includes 4 plug snaps)</li> <li>• Category 5 (CAT5) network cable</li> <li>• NXA-WAP250G Installation Guide</li> <li>• WallMount/Surface mounting installation kit (including two screws)</li> </ul>

### Power Connector

The access point does not have a power switch. It is powered on when connected to the AC power adapter, and the power adapter is connected to a power source. The power adapter automatically adjusts to any voltage between 100-240 volts at 50 or 60 Hz. No voltage range settings are required.

### Ethernet Port

The access point has one 10BASE-T/100BASE-TX RJ-45 port that can be attached directly to 10BASE-T/100BASE-TX LAN segments. These segments must conform to the IEEE 802.3-2005 specifications.

This port supports automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs, switches, or hubs.

### Reset Button

The Reset button is used to restart the access point or restore the factory default configuration. If you hold down the button for less than 5 seconds, the access point will perform a hardware reset. If you hold down the button for 5 seconds or more, any configuration changes you may have made are removed, and the factory default configuration is restored to the access point.



# Installation

## Overview

To install the Access Point, follow these steps:

1. **Select a Site** – Choose a proper place for the access point. For optimum performance, consider these points:
  - Mount the access point as high as possible above any obstructions in the coverage area. Avoid mounting next to or near building support columns or other obstructions.
  - Mount away from any signal absorbing or reflecting structures (such as those containing metal).
  - Avoid radio interference by mounting away from other 802.11b or g wireless devices.
2. **Mount the Access Point** – The access point is designed to be mounted on any horizontal surface, such as a desktop, or on a wall. The access point can be mounted on a wall by marking the position of the mounting screws (included) on the wall so they line up with the two mounting slots on the bottom of the access point. Set the screws into the wall, leaving about 3 mm (0.12 in.) clearance from the wall. Then slide the access point down onto the screws.
3. **Connect the Power Cord** – Connect the power adapter to the access point, and plug the power adapter into an AC power outlet.



*Use **ONLY** the power adapter supplied with the access point. Otherwise, the product may be damaged.*

CAUTION

4. **Observe the Indicator LEDs** – When you power on the access point verify that the POWER LED turns on and that the other LED indicators start functioning.
5. **Connect the Ethernet Cable** – The access point can be connected to any 10 or 100 Mbps Ethernet network device, such as a hub or a switch. Connect your network to the RJ-45 port on the back panel using category 3, 4, or 5 UTP Ethernet cable. When the access point and the connected device are powered on, the LAN LED should turn on indicating a valid network connection. If the LAN LED fails to turn on, refer to the *Appendix A: Troubleshooting* section on page 43.



*The RJ-45 port on the access point supports automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs, switches, or hubs.*

NOTE

## Access Point Configuration

The access point can be configured by connecting a PC to its Ethernet port and accessing the web interface.

The default IP address of the access point is 192.168.1.240, with login user name “Admin” and default password “1988”.

## Twisted-Pair Cable Assignments

For 10/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.



*Each wire pair must be attached to the RJ-45 connectors in a specific orientation. (See “Crossover Wiring” and “Crossover Wiring” for an explanation.)*

*DO NOT plug a phone jack connector into the RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.*

The following figure illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

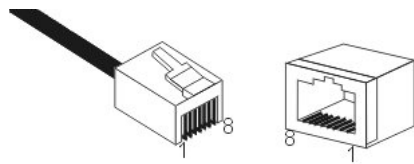


FIG. 2 RJ-45 connector pinouts

## Straight-Through Wiring

If the twisted-pair cable is to join two ports and only one of the ports has an internal crossover (MDI-X), the two pairs of wires must be straight-through. FIG. 3 diagrams the RJ-45 pinouts and signals for the Ethernet RJ-45 connector and cable.

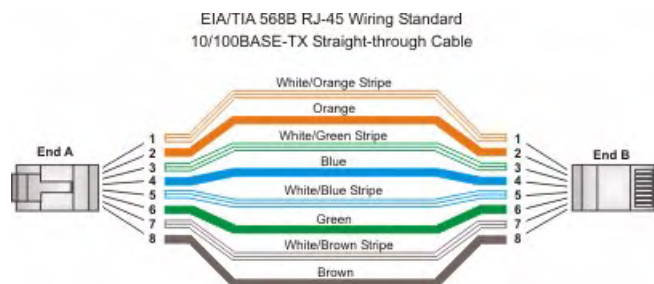


FIG. 3 Straight-Through Wiring

## Hardware Description

FIG. 7 shows the layout of the WAP250G connectors and components.

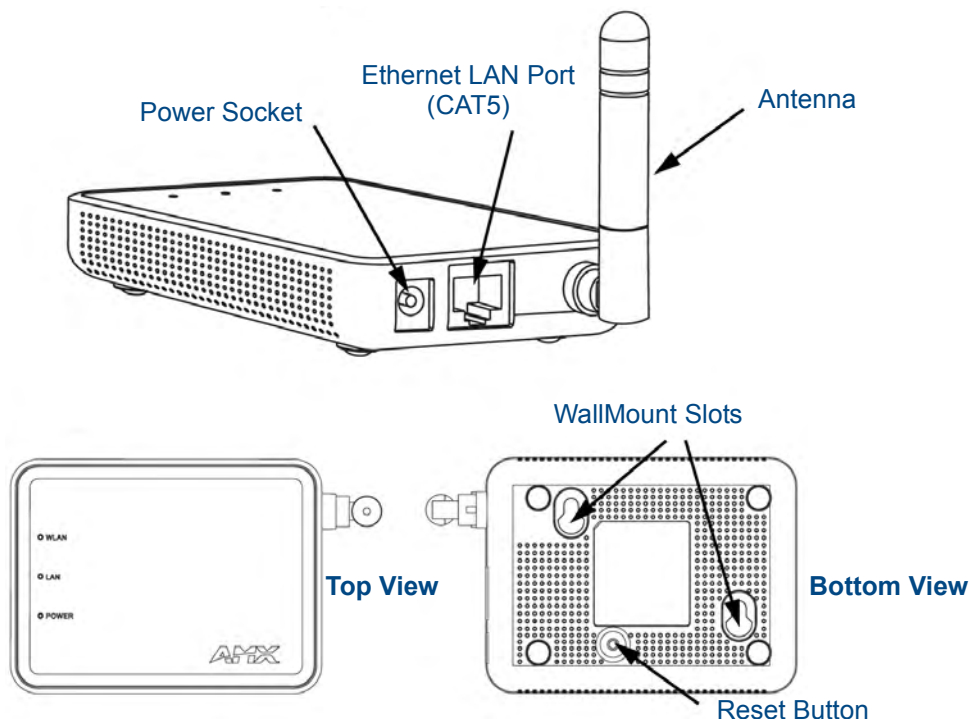


FIG. 4 NXA-WAP250G Component Locations

### Reset Button Overview

The Reset Button (shown in FIG. 7) is used to either restart the WAP250G or restore the unit to its factory default settings.

- If you hold down the button for **less than 5 seconds**, the WAP will perform a hardware reset.
- If you hold down the button for **more than 5 seconds**, any current configuration changes and settings (such as IP Address, MAC Address, security, etc.) are deleted and all of the unit's parameters are reset to the factory default settings.

### LED Indicators

The access point includes three status LED indicators, as described in the following figure and table.

LED	Status	Description
POWER	On Green	Indicates that the system is working normally.
WLAN	On/Flashing Green	Indicates the 802.11g radio is enabled and transmitting or receiving data through wireless links. The flashing rate is proportional to network activity.
	Off	Indicates the 802.11g radio is disabled.
LAN	On/Flashing Green	Indicates a valid link on the Ethernet port and that the access point is transmitting or receiving data. The flashing rate is proportional to network activity.
	Off	The Ethernet port has no valid link.

## Diagnosing Access Point Indicators

Symptom	Action
POWER LED is Off	<ul style="list-style-type: none"><li>• AC power adapter may be disconnected. Check connections between the access point, the power adapter, and the wall outlet.</li></ul>
LAN LED is Off	<ul style="list-style-type: none"><li>• Verify that the access point and attached device are powered on.</li><li>• Be sure the cable is plugged into both the access point and corresponding device.</li><li>• Verify that the proper cable type is used and its length does not exceed specified limits.</li><li>• Check the cable connections for possible defects. Replace the defective cable if necessary.</li></ul>

# Initial Configuration

The NXA-WAP250G offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer (version 6.0 or above).

The initial configuration steps can be made through the web browser interface using the Setup Wizard. It is recommended to make the initial changes by connecting a PC directly to the NXA-WAP250G before installing it in its intended location. The NXA-WAP250G has a default IP address of 192.168.1.240 and a subnet mask of 255.255.255.0. If your PC has an IP address on the same subnet (that is, the PC and NXA-WAP250G addresses both start 192.168.1.x), you can connect immediately to the web interface. Otherwise, you must first change your PC's IP address to be on the same subnet as the NXA-WAP250G.

The NXA-WAP250G can operate in one of two modes:

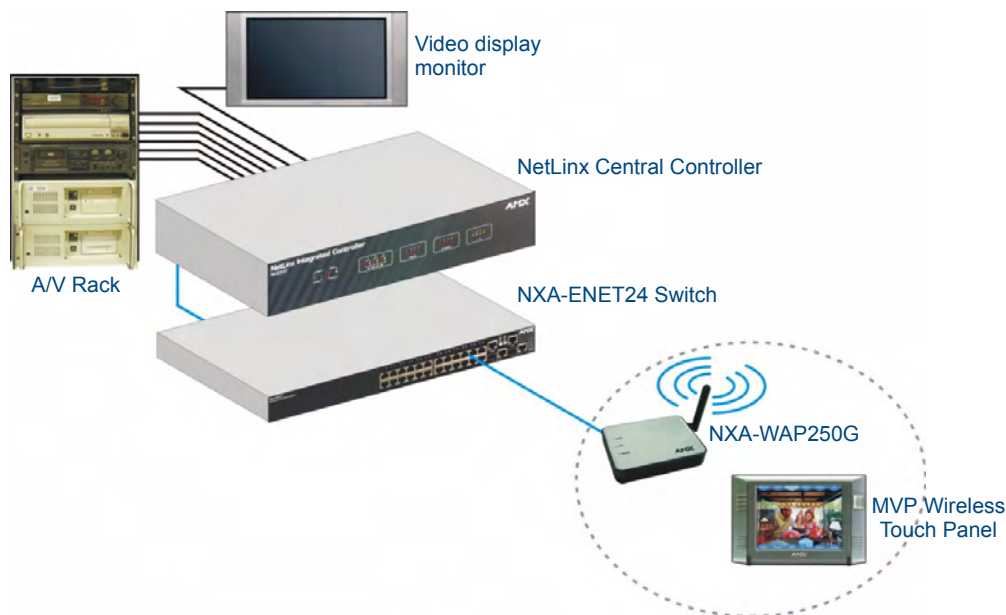
- **Access Point** – Providing connectivity to wireless clients in the service area.
- **Repeater and Bridge** – Providing an extended link to a remote access point from the wired LAN. Access Point working in this mode could connect to another AP in Access Point mode or Repeater and Bridge mode. Whenever there are two APs having wireless link together (one in Access Point or Repeater and Bridge mode, another using Repeater and Bridge mode), and also have wired link separately, these two APs are also working as “bridging” for the two wired links.

In addition, the NXA-WAP250G offers full network management capabilities through an easy to configure web interface.

## Selecting an Operation Mode

### Access Point Mode

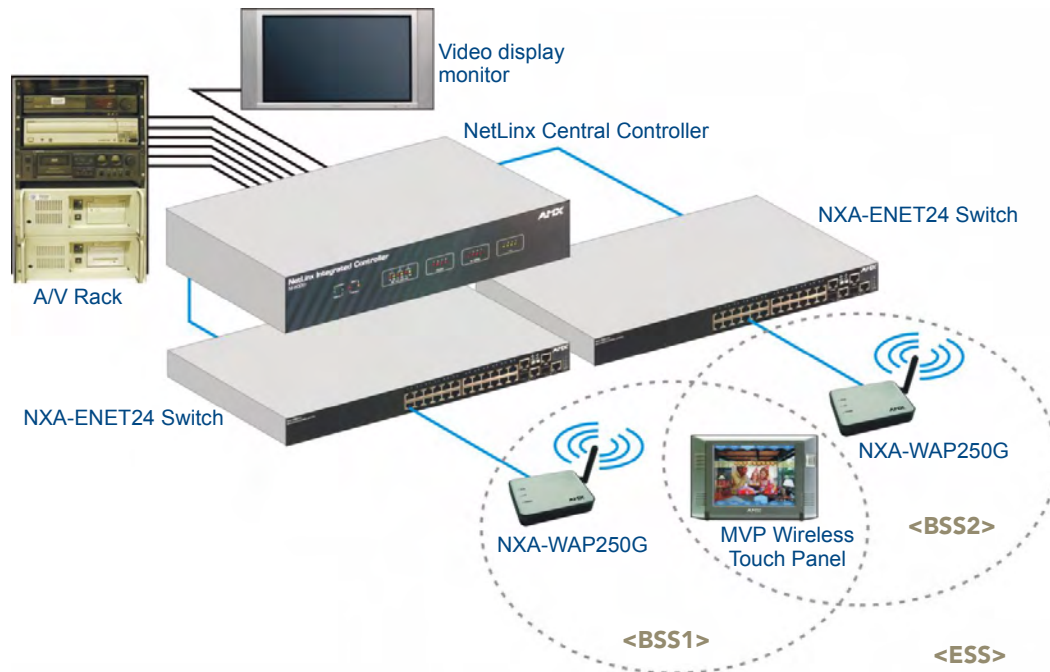
The NXA-WAP250G provides access to a wired LAN for wireless stations (FIG. 1). The wireless network is defined by a name, called the Service Set Identifier (SSID). All wireless stations must have the same SSID, radio channel, and security settings as the NXA-WAP250G to be able to communicate.



**FIG. 1** Access Point Mode - wired LAN for wireless stations

### Access Point Mode - Roaming

A wireless network can also support roaming for mobile users (FIG. 2). Multiple NXA-WAP250Gs can be placed so that a continuous coverage area is created. Wireless users within this area can move freely and remain connected to the network. All NXA-WAP250Gs and wireless stations in the network must be configured with the same SSID. Neighboring NXA-WAP250Gs should be set to non-interfering radio channels (that is, channels 1, 6, or 11 for 802.11b/g).

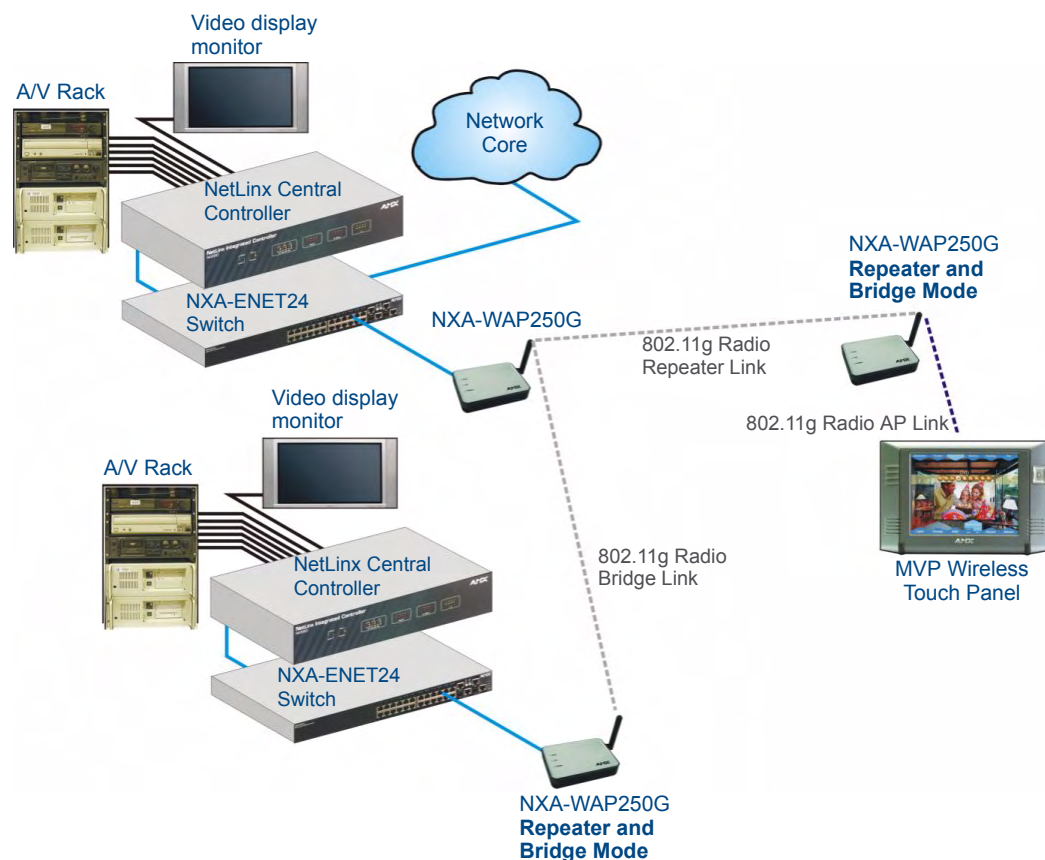


**FIG. 2** Access Point Mode - roaming for mobile users

### Access Point Mode - Repeater and Bridge Mode

The NXA-WAP250G can also operate in a “repeater and bridge” mode to extend the range of links to wireless clients (FIG. 3). The NXA-WAP250G uses Wireless Distribution System (WDS) to forward traffic between the repeater and the root access point. WDS is defined in the IEEE 802.11 standard for wireless connections between NXA-WAP250Gs.

In repeater and bridge mode, the NXA-WAP250G supports an Ethernet link to a wired LAN. Note that when the NXA-WAP250G operates in this mode only half the normal throughput is possible. This is because the NXA-WAP250G has to receive and then re-transmit all data on the same channel. Once an AP is configured as repeater, it could connect to another AP working in Access Point mode or Repeater and Bridge mode. In a deployed topology that has a repeater and bridge AP involved, there should be one AP working in Access Point mode.



**FIG. 3** Access Point Mode - Repeater and Bridge Mode



## Logging into the Web Interface

In the web browser's address bar, type the default IP address: **http://192.168.1.240**. The web browser displays the NXA-WAP250G's login page.

The User ID is fixed as **"Admin"** (case-sensitive), and the default password is **"1988"** (FIG. 4).

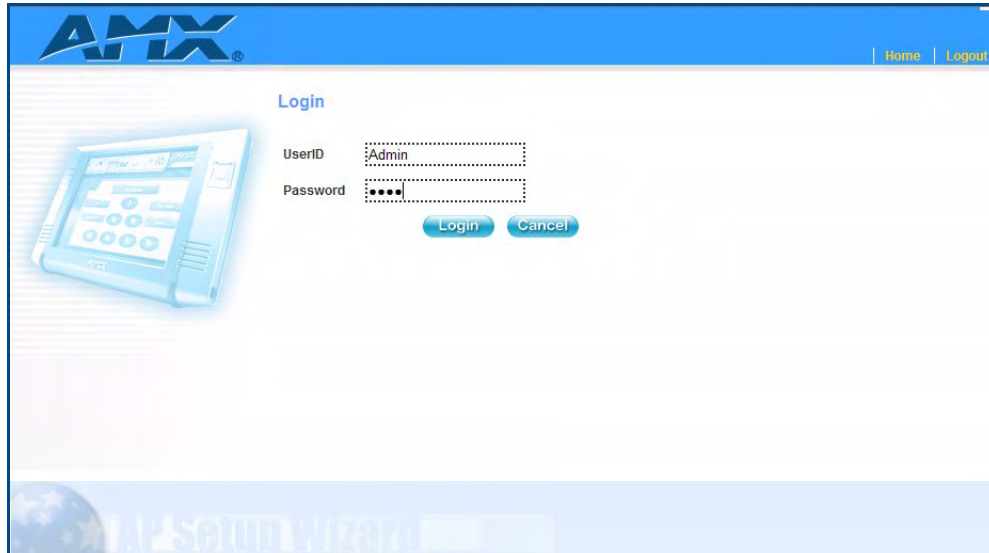


FIG. 4 Login Page



*It is strongly recommended that you configure a password. If a password is not configured, the management interface is not protected and anyone that can connect to the NXA-WAP250G may be able to compromise your network security. For information on configuring a password, see the System Setting - Administration section on page 26*

The home page displays the Main Menu (FIG. 5). There are two options available, you can configure the basic features of the NXA-WAP250G using the Setup Wizard's simple steps, or you can configure all features in detail using the Advanced Setup menu.

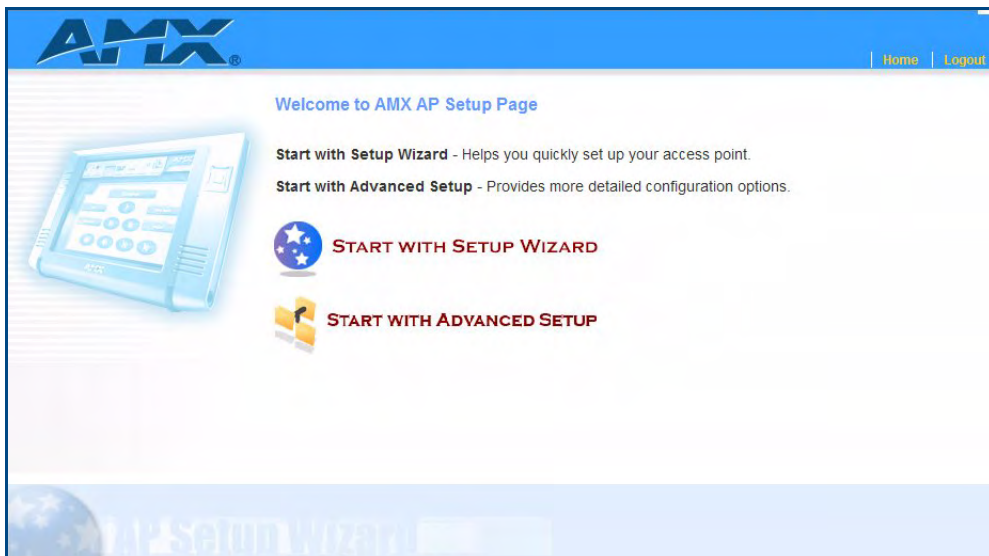


FIG. 5 Home Page



## Using the Setup Wizard

There are only a few basic steps you need to set up the NXA-WAP250G and provide a connection for your AMX Control Panel and network access for other wireless devices.

The Setup Wizard takes you through configuration procedures for the general network settings, such as IP configuration, wireless network name (Service Set Identifier), and wireless security. Follow these steps:

To begin, login and select **Start with Setup Wizard** on the home page (FIG. 5).

### Step 1: Operation Mode Setting

Select an operation mode according to how the unit will be used in your network (FIG. 6).

The figure displays two overlapping screenshots of the AMX Setup Wizard interface, specifically the 'Step 1: Operation Mode setting' screen. The interface has a blue header with the AMX logo and 'Home' and 'Logout' links. A list on the left shows 'Step 1: Operation Mode setting'. The main content area lists two options: '1. AP: The device functions as an Access Point.' and '2. Repeater & Bridge: The device functions as a Repeater or Bridge.' In the top screenshot, the 'AP' radio button is selected. In the bottom screenshot, the 'Repeater & Bridge' radio button is selected. Below the options, there is a 'Root AP' section with a text input field containing '00:00:00:00:00:00' and a dropdown menu labeled 'Please select a root AP'. A 'Scan' button is located next to the dropdown. At the bottom right of each screenshot are 'Cancel' and 'Next' buttons.

FIG. 6 Setup Wizard - Operation Mode setting

There are two operation modes:

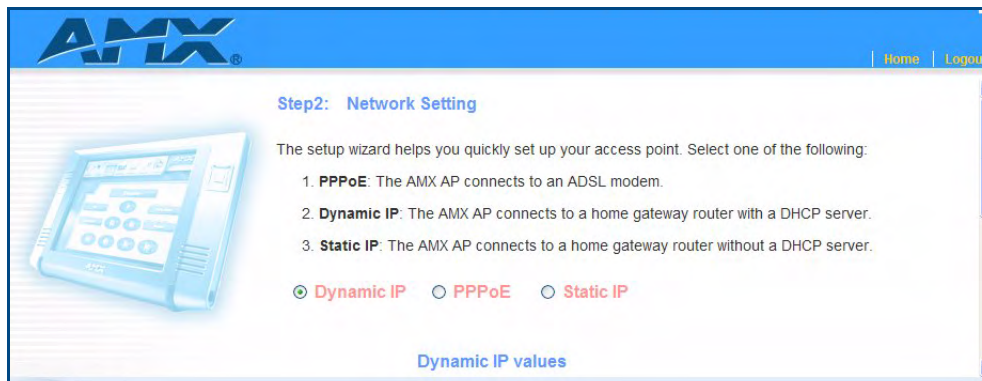
- **AP** — Set the device as an Access Point. The device can also act as a root bridge in a wireless bridge network.
- **Repeater & Bridge** — Set the device as a Wireless Repeater. The *Root AP MAC Address* can be assigned manually or selected after clicking **Scan**.

Reboot the NXA-WAP250G after completing the settings.

Click **Next** to proceed.

## Step 2: Network Setting

The options on this page allow you to set the NXA-WAP250G's IP address assignment method and configures the local Dynamic Host Configuration Protocol (DHCP) server and Network Address Translation (NAT) settings (FIG. 7).



**AMX** Home Logout

**Step2: Network Setting**

The setup wizard helps you quickly set up your access point. Select one of the following:

1. **PPPoE**: The AMX AP connects to an ADSL modem.
2. **Dynamic IP**: The AMX AP connects to a home gateway router with a DHCP server.
3. **Static IP**: The AMX AP connects to a home gateway router without a DHCP server.

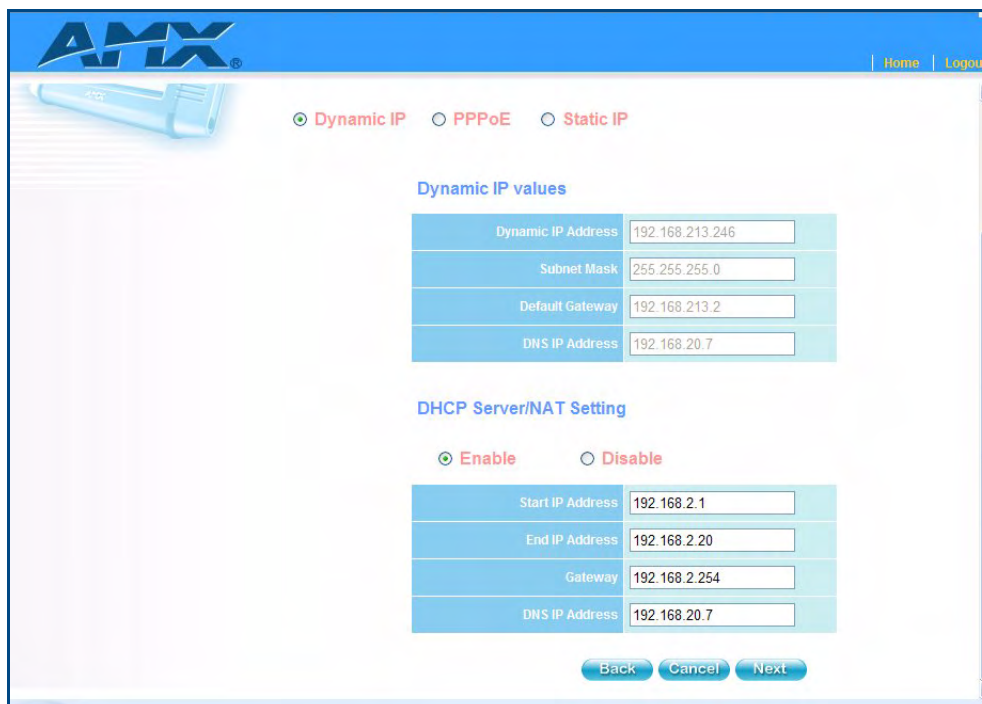
☒ Dynamic IP ☐ PPPoE ☐ Static IP

Dynamic IP values

FIG. 7 Setup Wizard - Network Setting

There are three basic methods for configuring the NXA-WAP250G's IP address:

- **Dynamic IP** — The IP address is assigned automatically from a home gateway router or other device that has a DHCP server feature (FIG. 8).



**AMX** Home Logout

☒ Dynamic IP ☐ PPPoE ☐ Static IP

Dynamic IP values

Dynamic IP Address	192.168.213.246
Subnet Mask	255.255.255.0
Default Gateway	192.168.213.2
DNS IP Address	192.168.20.7

DHCP Server/NAT Setting

☒ Enable ☐ Disable

Start IP Address	192.168.2.1
End IP Address	192.168.2.20
Gateway	192.168.2.254
DNS IP Address	192.168.20.7

Back Cancel Next

FIG. 8 Setup Wizard - Network Setting (Dynamic IP settings)

- **PPPoE** — The IP address is assigned automatically from an Internet service provider (ISP) through an ADSL modem using Point-to-Point Protocol over Ethernet (PPPoE). If your ISP has provided you with a user name and password, enter these in the corresponding text boxes under PPPoE Setting (FIG. 9).

AMX®

Home | Logout

☐ Dynamic IP
 ☒ PPoE
 ☐ Static IP

**PPoE Setting**

Username	<input type="text"/>
Password	<input type="text"/>

**DHCP Server/NAT Setting**

☒ Enable
 ☐ Disable

Start IP Address	192.168.2.1
End IP Address	192.168.2.20
Gateway	192.168.2.254
DNS IP Address	192.168.20.7

Back Cancel Next

**FIG. 9** Setup Wizard - Network Setting (PPoE settings)

- Static IP** — The IP address is assigned manually by the user. This may be required if your NXA-WAP250G is connected to a home gateway router or other device that does not support a DHCP server (FIG. 10).

AMX®

Home | Logout

☐ Dynamic IP
 ☐ PPoE
 ☒ Static IP

**Static IP Setting**

Static IP Address	192.168.213.246
Subnet Mask	255.255.255.0
Default Gateway	192.168.213.2
DNS IP Address	192.168.20.7

**DHCP Server/NAT Setting**

☒ Enable
 ☐ Disable

Start IP Address	192.168.2.1
End IP Address	192.168.2.20
Gateway	192.168.2.254
DNS IP Address	192.168.20.7

Back Cancel Next

**FIG. 10** Setup Wizard - Network Setting (Static IP settings)

- If you select Static IP, enter an appropriate IP address and subnet mask that are compatible with your existing network.
- If a management station exists on another network segment, then you must enter the IP address for a Default Gateway that can route traffic between these segments.

- Also enter the IP address for the Domain Name Server (DNS) to be used for host-name to IP address resolution.

### DHCP Server/NAT Setting

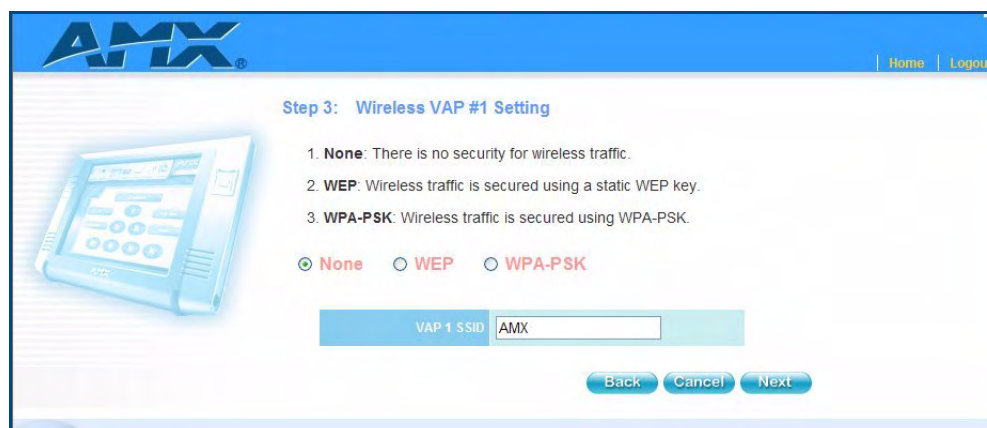
The NXA-WAP250G includes a DHCP server that can assign IP addresses to any wireless device. Addresses are assigned from a common address pool configured on the NXA-WAP250G. You can configure the address pool by specifying start and end IP addresses.

NAT is a standard method of mapping multiple “internal” IP addresses to one “external” IP address on devices at the edge of a network. For the NXA-WAP250G, the internal (local) IP addresses are the IP addresses assigned to wireless clients by the DHCP server, and the external IP address is the IP address assigned to the NXA-WAP250G itself. Note that the NXA-WAP250G IP address is always in a different subnet from the DHCP server pool. The NXA-WAP250G uses the NAT IP settings to route traffic from the wireless interface to the Ethernet network.

Click **Next** to proceed.

### Step 3: Wireless VAP #1 Setting

The options on this page for VAP (Virtual Access Point) #1 set the wireless Service Set Identifier (SSID) and wireless security encryption key for the VAP#1 network (FIG. 11).



**FIG. 11** Setup Wizard - Setting the VAP#1 SSID and Security

- It is recommended to restrict one VAP network for only AMX Control Panels and let all other wireless devices use the other VAP network or the second SSID.
- VAP1 provides higher priority for wireless communications associated with this SSID, relative to the second SSID (VAP2).

Enter the SSID, or wireless network name, which all wireless stations must use to associate with the NXA-WAP250G. The SSID is case sensitive and can consist of up to 32 alphanumeric characters (default: **Wireless Network - 1**).

The NXA-WAP250G offers two wireless security options;

- Wired Equivalent Privacy (**WEP**)
- Wi-Fi Protected Access Pre-shared Key (**WPA-PSK**)

Select the security you want to use and enter the appropriate encryption key (or select **None** for no security).

- **WEP Key** - Enter 10 hexadecimal digits (0 to 9 and A to F) or 5 alphanumeric characters for 64 bit keys, 26 hexadecimal digits or 13 alphanumeric characters for 128 bit keys, and 32 hexadecimal digits or 16 alphanumeric characters for 152 bit keys (FIG. 12).



[Home](#) | [Logout](#)

---

### Step 3: Wireless VAP #1 Setting



1. **None**: There is no security for wireless traffic.

2. **WEP**: Wireless traffic is secured using a static WEP key.

3. **WPA-PSK**: Wireless traffic is secured using WPA-PSK.

☐ None  
 ☒ **WEP**  
 ☐ WPA-PSK

VAP 1 SSID

WEP key

**FIG. 12** Setup Wizard - Wireless VAP #1 Setting (WEP settings)

- WPA-PSK Key** — Enter as an easy-to-remember form of letters and numbers. The key must be from 8 to 63 characters, which can include spaces (FIG. 13).



[Home](#) | [Logout](#)

---

### Step 3: Wireless VAP #1 Setting



1. **None**: There is no security for wireless traffic.

2. **WEP**: Wireless traffic is secured using a static WEP key.

3. **WPA-PSK**: Wireless traffic is secured using WPA-PSK.

☐ None  
 ☐ WEP  
 ☒ **WPA-PSK**

VAP 1 SSID

WPA-PSK key

**FIG. 13** Setup Wizard - Wireless VAP #1 Setting (WPA-PSK settings)



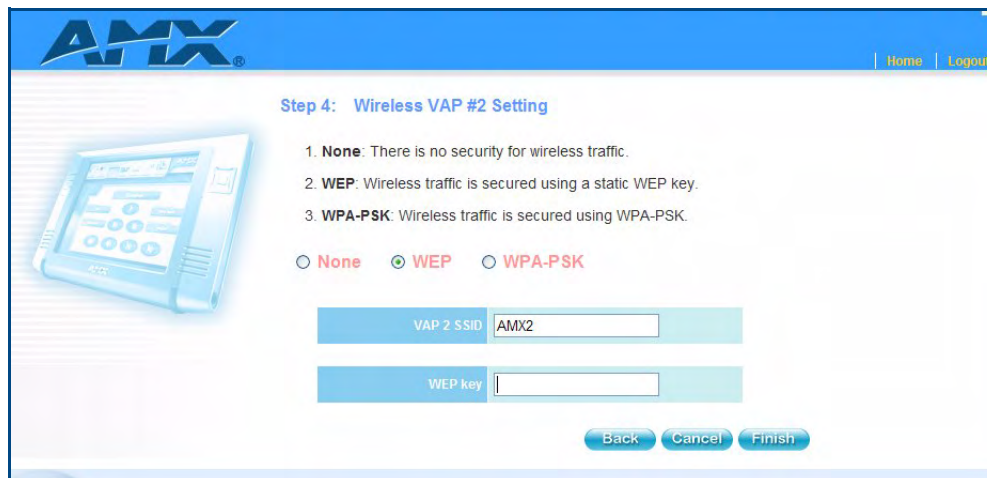
*All wireless devices must be configured with the same WEP or WPA-PSK Key values to communicate with the NXA-WAP250G.*

Click **Next** to proceed.



### Step 4: Wireless VAP #2 Setting

The options on this page allow you to set the wireless Service Set Identifier (SSID) and wireless security encryption key for the VAP#2 wireless network (FIG. 14).



**AMX** Home Logout

**Step 4: Wireless VAP #2 Setting**

1. **None**: There is no security for wireless traffic.  
 2. **WEP**: Wireless traffic is secured using a static WEP key.  
 3. **WPA-PSK**: Wireless traffic is secured using WPA-PSK.

☐ None ☒ WEP ☐ WPA-PSK

VAP 2 SSID:

WEP key:

Back Cancel Finish

**FIG. 14** Setup Wizard - Wireless VAP #2 Setting



*Wireless VAP #2 Setting is only available when the Operation Mode is set to **AP** (see FIG. 6 on page 13).*

Enter the SSID, or wireless network name, which all wireless stations must use to associate with the NXA-WAP250G. The SSID is case sensitive and can consist of up to 32 alphanumeric characters (Default: Wireless Network - 2).



*Both SSIDs (VAP#1 and VAP#2) must use the same encryption method.*

The NXA-WAP250G offers two wireless security options; Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access Pre-shared Key (WPA-PSK). Select the security you want to use and enter the appropriate encryption key, or select “None” for no security.

- **WEP Key** — Enter 10 hexadecimal digits (0 to 9 and A to F) or 5 alphanumeric characters for 64 bit keys, 26 hexadecimal digits or 13 alphanumeric characters for 128 bit keys, and 32 hexadecimal digits or 16 alphanumeric characters for 152 bit keys.
- **WPA-PSK Key** — Enter as an easy-to-remember form of letters and numbers. The key must be from 8 to 63 characters, which can include spaces.

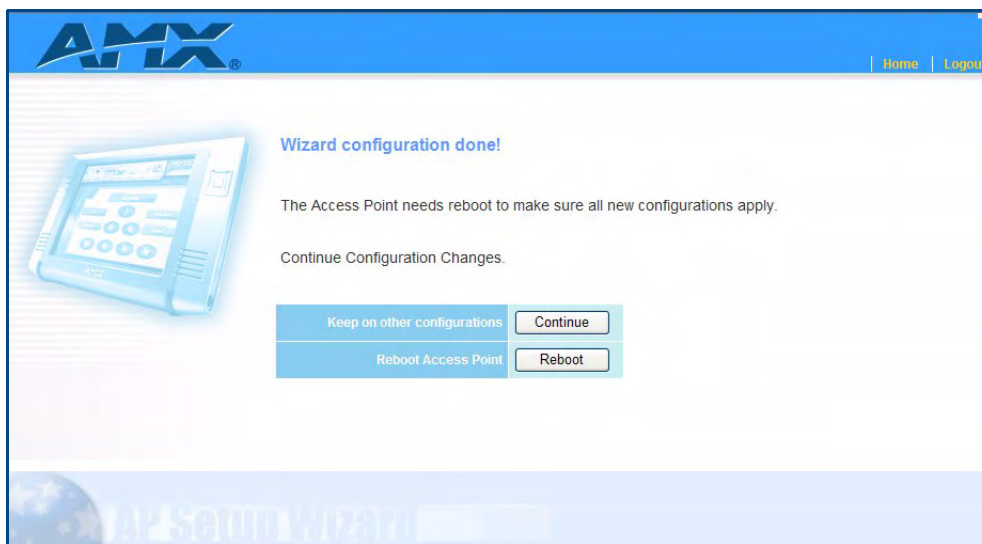


*All wireless devices must be configured with the same WEP or WPA-PSK Key values to communicate with the NXA-WAP250G.*

Click **Next** to proceed.

## Finish and Reboot

1. Click **Finish** (FIG. 15).



**FIG. 15** Setup Wizard - Wizard configuration done

2. Click the **Reboot** button to restart the NXA-WAP250G.

Rebooting of the NXA-WAP200G can take up to 90 seconds.



*The NXA-WAP250G will start using any configured new IP settings, which must be used to access the web management interface.*



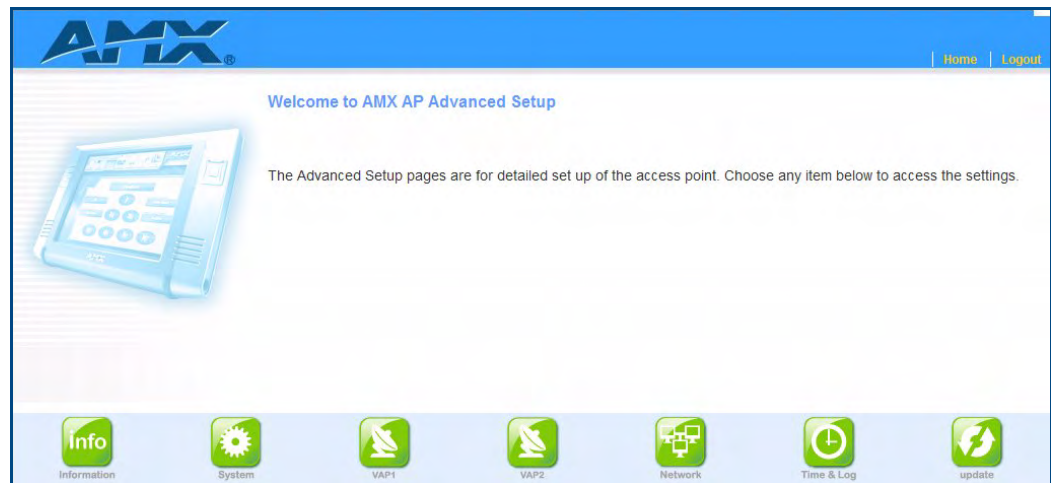


# System Configuration

The NXA-WAP250G's basic settings can be configured using the Setup Wizard, as described in the previous chapter, "Initial Configuration." However, for some installations, you may need to configure specific settings that are not available in the Setup Wizard. The Advanced Setup menu provides access to all the unit's settings for complete control of the WAP250G's features.

To access the Advanced Setup menus, follow these steps:

1. Login to the web interface (see the *Logging into the Web Interface* section on page 12).
2. When the Home page opens, select **Advanced Setup**. The *Welcome to AMX AP Advanced Setup* page displays (FIG. 16).



**FIG. 16** Advanced Setup

The information in this chapter is organized to reflect the structure of the web management screens for easy reference. However, it is recommended that you first configure a password to control access to the management interface. For details, see the *System Setting - Administration* section on page 26.

The Advanced Setup pages include the options in the table below. For details on configuration for each feature, see the corresponding page number.

Configuration Options		
Menu	Description	Page
<b>Information</b>		
System	Displays a summary of WAP250G settings	23
Client	Displays information on stations associated to the WAP250G	24
Network	Displays DHCP client, server, NAT, and PPPoE settings	25
Event Log	Displays the system message log	25
<b>System</b>		
Administration	Configures the password for management access	26
Operation	Sets the device function	27
VAP Management	Manages the VAP's traffic and priority	28
Reboot System	Restarts the system and resets configuration settings to factory defaults	28

Configuration Options (Cont.)		
Menu	Description	Page
<b>Wireless VAP 1, 2 (Wireless VAP 2 is only available when the Operation Mode is set to AP)</b>		
Basic	Enables the VAP interface and sets the SSID	29
Channel	Sets the radio channel	30
WEP	Configures WEP security	31
WPA-PSK	Configures WPA-PSK security	33
<b>Network</b>		
DHCP Client	Enables DHCP client or manually sets an IP address	34
DHCP Server/NAT	Enables DHCP server and configures NAT settings	35
PPPoE	Configures PPPoE settings	36
<b>Time &amp; Log</b>		
SNTP	Sets the system clock using SNTP	38
<b>Update</b>		
Upgrade via the Web Page	Upgrades system software from a local file	39
Upgrade via a Remote Server	Upgrades system software from a file on an FTP or TFTP server	40

## Information

The *Information* pages display details on the current configuration and status of the WAP250G, including associated wireless stations and event log messages (FIG. 17).

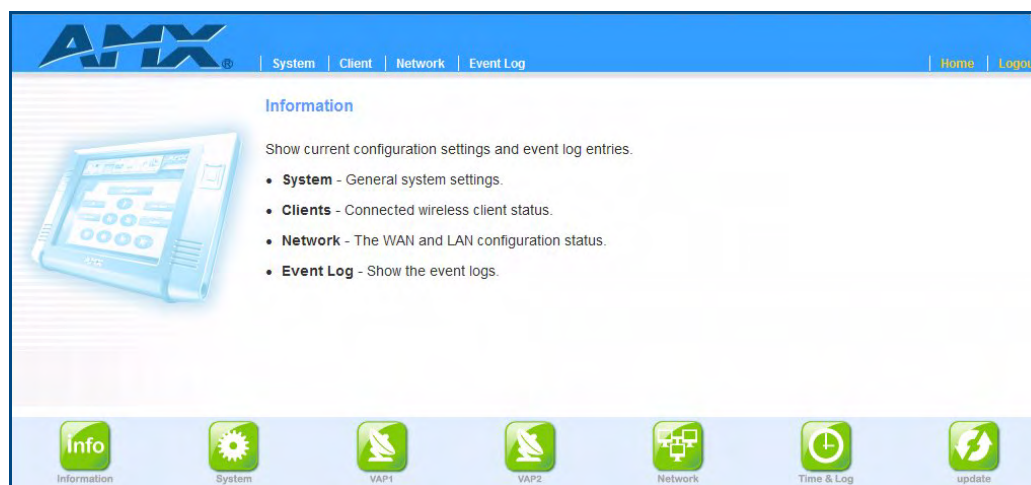


FIG. 17 Information page



*The items on the Information pages are for status display only, and are not configurable.*

## Information - System

The *System Information* page (FIG. 18) displays basic system configuration settings, as well as the settings for each wireless interface.



The screenshot displays the 'AP System Configuration' page. On the left is a small image of the WAP250G device. The main content area is divided into three sections: 'AP System Configuration', 'Wireless VAP #1 SSID Configuration', and 'Wireless VAP #2 SSID Configuration'. Each section contains a table of settings. At the bottom is a navigation bar with icons for Info, System, VAP1, VAP2, Network, Time & Log, and Update.

System Up Time	Day 0, 4:59:46
MAC Address	00-12-CF-2E-9A-8C
IP Address	192.168.213.246
IP default gateway	192.168.213.2
HTTP Server	Enabled
HTTP Server Port	80
VAP Management	Disabled
VLAN Status	Disabled
Version	v1.0.5.0

SSID	AMX
Broadcast SSID	Enabled
Channel	5
Radio Status	Enabled
Encryption	Enabled
Authentication Type	Open System
Multicast Cipher	WEP

SSID	AMX2
Broadcast SSID	Enabled
Radio Status	Enabled
Encryption	Enabled
Authentication Type	Open System
Multicast Cipher	WEP

FIG. 18 System Information

The items on this page include:

**AP System Configuration:** Displays basic system configuration settings:

- **System Up Time:** Length of time since the WAP250G was powered on.
- **MAC Address:** The physical layer address for the WAP250G's Ethernet port.
- **IP Address:** The IP address configured on the WAP250G.
- **IP Default Gateway:** The IP address of the gateway router between the WAP250G and management stations that exist on other network segments.
- **HTTP Server:** The status of the web management server.
- **HTTP Server Port:** The TCP port used by the web management server.
- **Version:** The version number of the current WAP250G software.

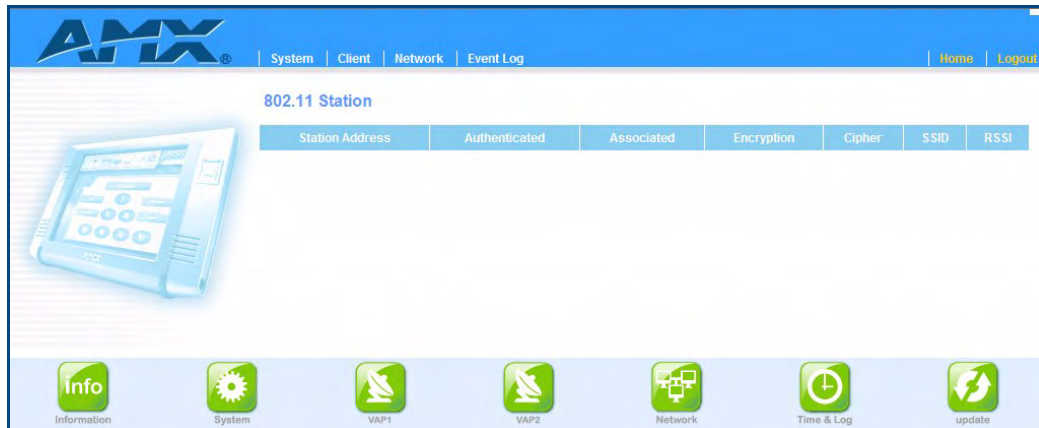
**Wireless Data #1/#2 SSID Configuration:** The AP Wireless Configuration table displays the wireless interface settings listed below.

- **SSID:** The service set identifier for this wireless group.
- **Channel:** The radio channel through which the WAP250G communicates with wireless clients.
- **The encryption status:** The key size used for data encryption.
- **Authentication Type:** Shows if open system or shared key authentication is used.

- **Multicast Cipher:** The encryption used for broadcast and multicast data.

### Information - Client

The *Client* page (FIG. 19) displays details on wireless devices currently associated to the WAP250G.



**FIG. 19** Client Information

The items on this page include:

- **Station Address:** The MAC address of the wireless client.
- **Authenticated:** Shows if the client has been authenticated. The two basic methods of authentication supported for 802.11 wireless networks are “open system” and “shared key.” Open-system authentication accepts any client attempting to connect to the WAP250G without verifying its identity. The shared-key approach uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to clients before attempting authentication.
- **Associated:** Shows if the client has been successfully associated with the WAP250G. Clients can associate with the WAP250G only after authentication has completed.
- **Encryption:** Indicates if encryption is being used by the client; either Enabled or Disabled.
- **Cipher:** Indicates the encryption cipher capability being advertised by the client; WEP, TKIP, AES, or None.
- **SSID** -- The VAP interface that the client is associated with.
- **RSSI** -- The received signal strength of the client.

## Information - Network

The *Network* page displays the current Dynamic Host Configuration Protocol (DHCP) client, DHCP server, and Point-to-Point Protocol over Ethernet (PPPoE) status (FIG. 20).

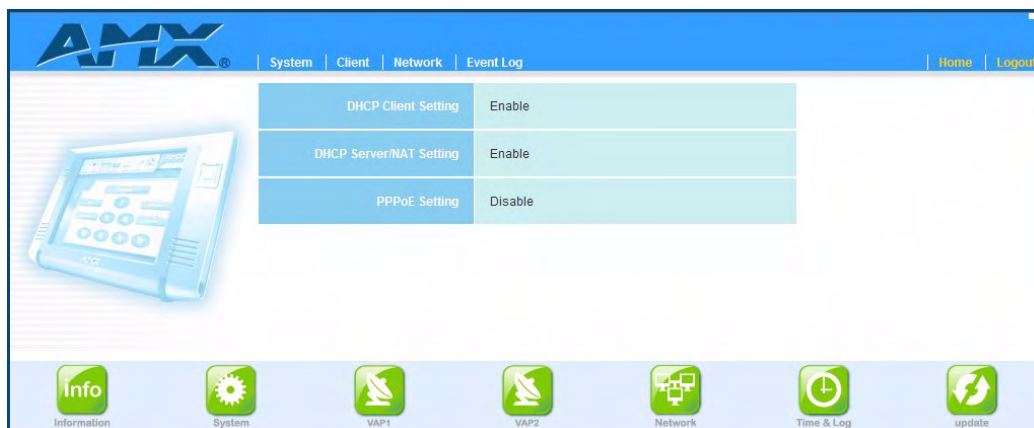


FIG. 20 Network Information

The items on this page include:

- DHCP Client Setting:** Enables the WAP250G to automatically obtain an IP address from a DHCP server. When disabled, or if a response is not received from the DHCP server, the WAP250G uses the configured static IP settings on the Network > DHCP Client page (default: *Disabled*).
- DHCP Server/NAT Setting:** Enables or disables the DHCP server on the WAP250G. The WAP250G DHCP server can assign IP addresses to any wireless client requesting the service. Addresses are assigned to clients from a common address pool configured on the Network > DHCP Server/NAT page (default: *Disabled*).
- PPPoE Setting:** Enables a connection to an Internet service provider using PPPoE. The PPPoE access user name and password can be set on the Network > PPPoE page (default: *Disabled*).

## Information - Event Log

The *Event Log* page displays system messages generated during system operation. The logged messages can serve as a valuable tool for isolating WAP250G and network problems (FIG. 21).

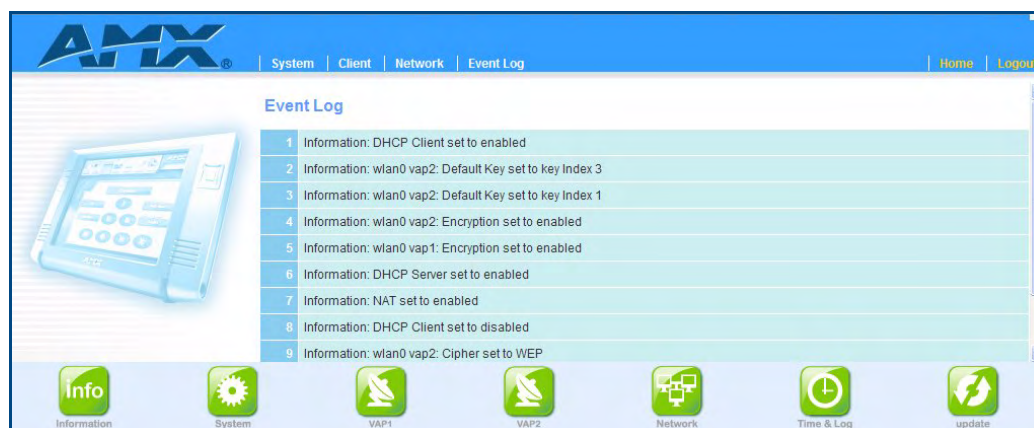


FIG. 21 Event Log



The Event Log page displays the last 128 messages logged in chronological order, from the newest to the oldest. Log messages saved in the WAP250G's memory are erased when the device is rebooted.

## System Setting

The *System Settings* pages allow you to change the management access password and restart the WAP250G (FIG. 22).

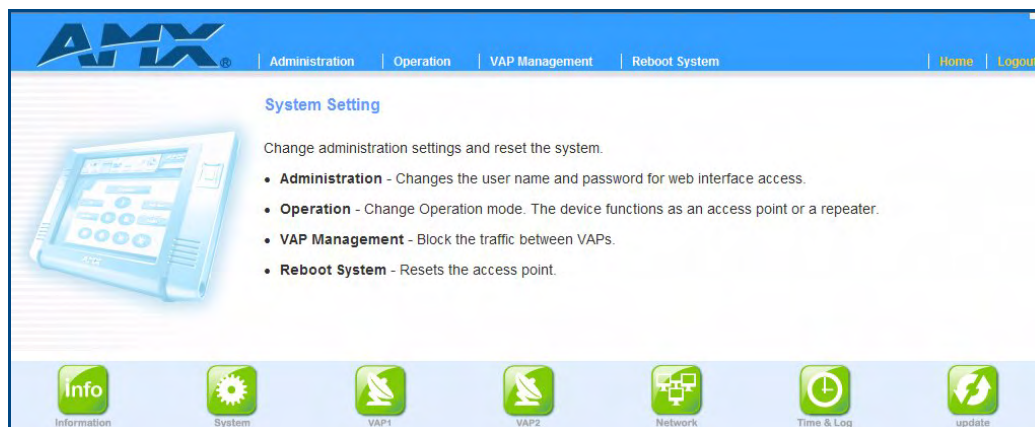


FIG. 22 System Setting

### System Setting - Administration

Management access to the WAP250G is controlled through a single password. Use the options on the *Administration Settings* page (FIG. 23) to change the user name and password for web interface access.

To protect access to the management interface, you need to configure an Administrator password as soon as possible. If the password is not configured, then anyone having access to the WAP250G may be able to compromise WAP250G and network security.

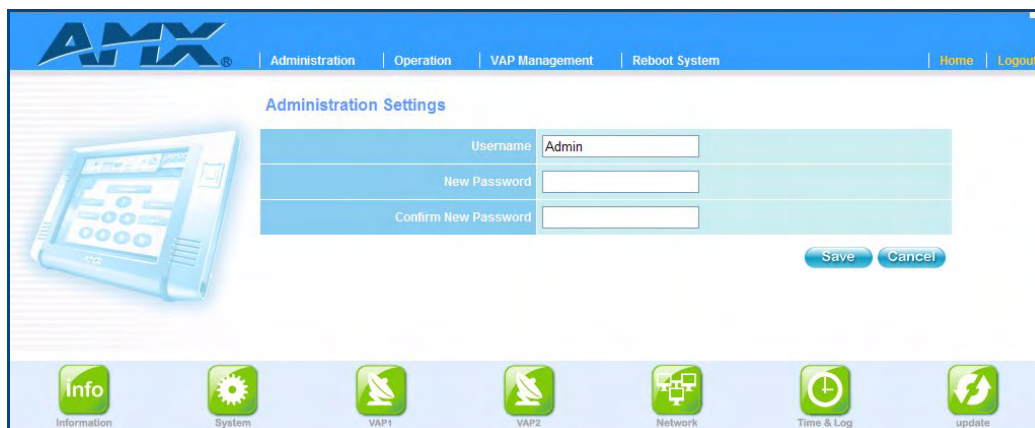


FIG. 23 System Settings - Administration Settings



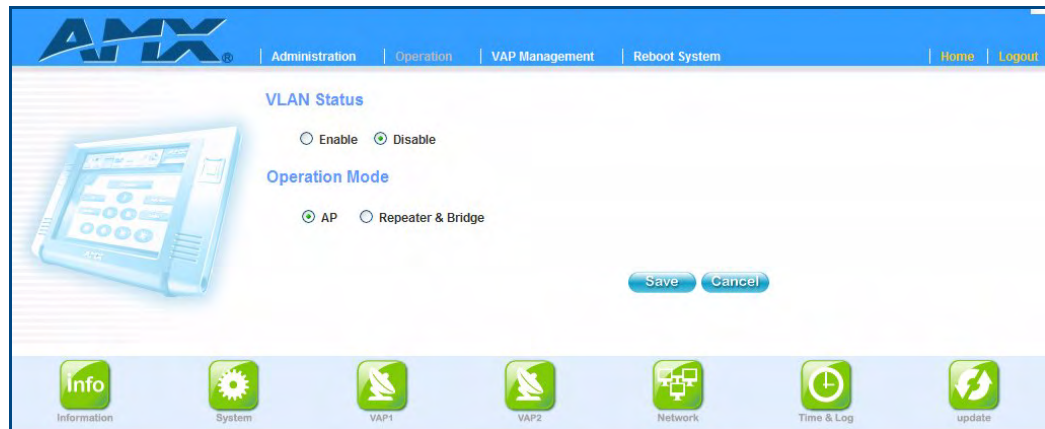
*Pressing the reset button on the back of the WAP250G for more than five seconds resets the user name and password to the factory defaults.*

The items on this page include:

- **Username:** The name of the user. The default username is “Admin” (case-sensitive) and is configurable.
- **New Password:** The password for management access. (Length: 0-32 characters, case sensitive)
- **Confirm New Password:** Enter the password again for verification.

### System Setting - VLAN Status / Operation Mode

The options on this page allow you to enable/disable *VLAN Status*, and specify the *Operation Mode*. The WAP250G can be set as an access point, a wireless repeater or a wireless bridge according to how you want to use the unit in your network (FIG. 24).



**FIG. 24** System Settings - Operation

**VLAN Status:** Click the **Enable** radio button to maintain VLAN (virtual LANs) on the WAP250G (default: *Disabled*).

VLANs represent a method of creating independent logical networks within a physical network. Several VLANs can co-exist within such a network. VLANs are commonly used to increase the number of broadcast domains while reducing the size of each broadcast domain, which in turn reduces network traffic and increases network security (both of which are hampered in cases of single large broadcast domains).

#### Operation Modes:

There are two **Operation Modes**:

- **AP** — Set the device as an Access Point. The device can also act as a root bridge in a wireless bridge network.
- **Repeater & Bridge** — Set the device as a Wireless Repeater and Bridge. The Root AP MAC Address can be configured manually or selected after clicking **Scan**.



*In Repeater & Bridge mode, the access point only connects to other NXA-WAP250G units.*

Reboot the WAP250G after completing the settings.

## System Setting - VAP Management

The VAP Management page allows you to enable VAP management (FIG. 25).

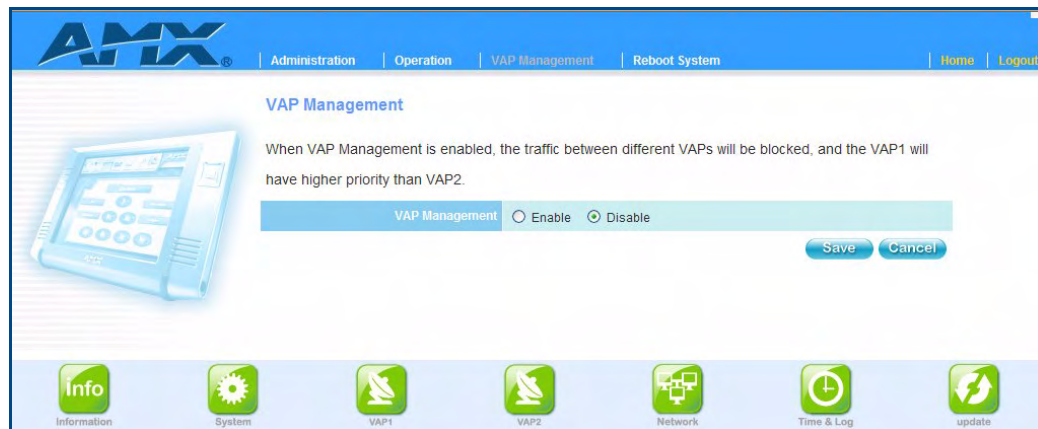


FIG. 25 System Settings - VAP Management

When VAP management is enabled, it tags traffic from VAP#1 as high priority and traffic from VAP#2 as low priority.



*This setting is only available when the Operation Mode is set to AP.*

## System Settings - Reset System

The Reset System page (FIG. 26) allows you to restart the WAP250G software and restore factory default settings.

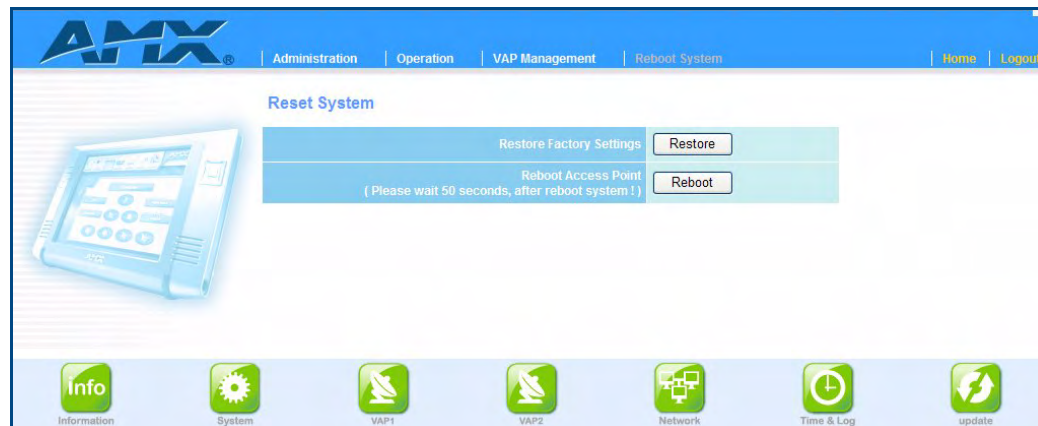


FIG. 26 System Settings - Reset System

The items on this page include:

- **Restore Factory Settings:** Click the Restore button to reset the configuration settings for the WAP250G to the factory defaults and reboot the system. Note that all user configured information will be lost. You will have to use the default IP address to re-gain management access to the WAP250G.
- **Reboot Access Point:** Click the Reboot button to reboot the system.





*If you have upgraded the system software, then you must reboot the WAP250G to implement the new code.*

## Wireless VAP Settings

The Wireless VAP #1 Setting and Wireless VAP #2 Setting pages include configuration options for radio signal characteristics and wireless security features on the WAP250G (FIG. 27).



FIG. 27 Wireless VAP 1 Setting - main page



*VAP #1 is only available when the Operation Mode is set as an AP.*

The following sections apply to both Wireless VAP #1 Setting and Wireless VAP #2 Setting pages.



*it is recommended to restrict one VAP network for only AMX Control Panels and let all other wireless stations use the other VAP network.*

### Wireless VAP Settings - Basic Setting

The *Basic Setting* page (FIG. 28) allows you to enable the VAP radio interface and define the Service Set Identifier (SSID).

The WAP250G includes an IEEE 802.11g radio for wireless communications. The IEEE 802.11g standard operates within the 2.4 GHz band at up to 54 Mbps. Note that because the IEEE 802.11g standard is an extension of the IEEE 802.11b standard, it allows clients with 802.11b wireless network cards to associate to an 802.11g access point.

The SSID is a recognizable text string that identifies the wireless network service provided by the VAP interface. Wireless clients that want to connect to the network must set their SSIDs to match that of the VAP interface.

The items on this page include:

- **Radio Status:** Enables radio communications for the VAP interface.  
(Defaults: VAP #1 - *Enabled*, VAP #2 - *Disabled*)

**AMX** Basic Channel WEP WPA / WPA2 Home Logout

### Wireless VAP1 Basic Setting

Radio Status: ☒ Enable ☐ Disable

SSID:

Broadcast SSID: ☒ Enable ☐ Disable

VLAN Id:

Client Access Mode: ☐ 802.11g only ☒ b+g

Save Cancel

Info System VAP1 VAP2 Network Time & Log update

**FIG. 28** Wireless VAP 1 Setting - Basic Settings

- **SSID:** The name of the wireless network service provided by the VAP. Clients that want to connect to the network must set their SSID to the same as that of the VAP interface. (Defaults: VAP #1 - *AMX1*, VAP #2 - *AMX2*; Range = 1-32 characters).
- **Broadcast SSID:** Enable this option to allow the WAP250G to transmit its SSID at regular intervals (every few seconds). This feature is intended to allow clients to dynamically discover and roam between WLANs.
- **VLAN Id:** Enter a unique 12-bit VLAN Id (or VID) for the WAP250G.
- **Client Access Mode:** Select the access mode to be used by the WAP250G (*802.11g only*, or *b+g*). By default, the access mode is set to **b+g**.

### Wireless VAP Settings - Channel Setting

The WAP250G uses one radio channel in the 2.4 GHz band to communicate with its clients. The radio channel may be set manually by the user or automatically by the system, which selects the channel with the least radio interference (FIG. 29).

**AMX** Basic Channel WEP WPA / WPA2 Home Logout

### Wireless VAP1 Channel Setting

Auto Channel Selection: ☒ Enable ☐ Disable

Radio Channel:

Save Cancel

Info System VAP1 VAP2 Network Time & Log update

**FIG. 29** Wireless VAP 1 Setting - Channel Setting



**NOTE**

*If you experience poor performance, you may be encountering interference from another wireless device. Try changing the channel, as this may eliminate interference and increase performance. Channels 1, 6, and 11, as the three non-overlapping channels in the 2.4 GHz band, are preferred. Using channels other than 1, 6, and 11 can cause degraded performance.*

The items on this page include:

- **Auto Channel Selection:** Enables the WAP250G to automatically select an interference-free radio channel (default: *Enabled*).
- **Radio Channel:** The radio channel that the WAP250G uses to communicate with wireless clients. When multiple WAP250Gs are deployed in the same area, set the channel on neighboring WAP250Gs at least five channels apart to avoid interference with each other.

For example, you can deploy up to three WAP250Gs in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the WAP250G to which it is linked (range = 1-11; default = 11).

### Wireless VAP Settings - WEP Setting

The WAP250G is configured by default as an “open system,” which broadcasts a beacon signal including the configured SSID. Wireless clients with a configured SSID of “any” can read the SSID from the beacon and automatically set their SSID to allow immediate connection to the WAP250G. To secure the wireless network, you have to implement user authentication and wireless data encryption.

Wired Equivalent Privacy (WEP) provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the WAP250G. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network (FIG. 30).

**AMX** | Basic | Channel | WEP | WPA / WPA2 | Home | Logout

#### Wireless VAP1 WEP Setting

WEP Status	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Authentication Mode	<input checked="" type="radio"/> Open	<input type="radio"/> Shared
Key Source	<input checked="" type="radio"/> Static config	<input type="radio"/> Dynamic from Radius
Key Type	<input checked="" type="radio"/> Hexadecimal	<input type="radio"/> Alphanumeric

Setting Key(These 4 WEP keys are shared between both VAPs)

<input checked="" type="radio"/> Key 1	<input checked="" type="radio"/> 64 Bit <input type="radio"/> 128 <input type="radio"/> 152	*****
<input type="radio"/> Key 2	<input checked="" type="radio"/> 64 Bit <input type="radio"/> 128 <input type="radio"/> 152	
<input type="radio"/> Key 3	<input checked="" type="radio"/> 64 Bit <input type="radio"/> 128 <input type="radio"/> 152	*****
<input type="radio"/> Key 4	<input checked="" type="radio"/> 64 Bit <input type="radio"/> 128 <input type="radio"/> 152	

Save Cancel

Info System VAP1 VAP2 Network Time & Log update

FIG. 30 Wireless VAP 1 Setting - WEP Security

The items on this page include:

- **WEP Status:** Enables the WAP250G to use WEP shared keys. If enabled, you must configure at least one key for the VAP interface and all its clients.
- **Authentication Mode:** Select *Open* or *Shared*.

With Authentication Mode set to **Open**, any bridge can authenticate and then attempt to communicate with the WAP250G. If the WAP250G is using WEP and the other bridge is not, the other bridge does not attempt to authenticate. If the other bridge is using WEP but its WEP keys do not match the keys on the WAP250G, the other bridge authenticates with the WAP250G but does not pass data through it.

With Authentication Mode set to **Shared**, the WAP250G sends an unencrypted challenge string to any bridge attempting to communicate with the WAP250G. The bridge

requesting authentication encrypts the challenge text and sends it back to the WAP250G. If the challenge text is encrypted correctly, the access point enables the requesting bridge to authenticate.

- *Shared* authentication mode is less secure than *Open* due to the unencrypted / encrypted string handshake.
- Only one SSID can use *Shared* authentication.



*Although an access point can use the EAP method to authenticate a wireless client device, an access point cannot use EAP to authenticate another access point. In other words, bridges must authenticate each other using either Open or Shared authentication methods.*

- **Key Source:** Select *Static config* or *Dynamic from Radius*. *Static config* is for use with WEP, *Dynamic from Radius* is for use with WPA.
- **Key Type:** Select the preferred method of entering WEP encryption keys on the WAP250G.
  - **Hexadecimal:** Enter keys as hexadecimal digits (0 to 9 and A to F).
  - **Alphanumeric:** Enter keys as alphanumeric characters.
- **Setting Key:** Sets WEP key values for one or two keys. At least one key must be specified. Each WEP key has an index number. Index numbers 1 and 2 apply to VAP #1 interface and numbers 3 and 4 apply to VAP #2 interface. The selected key is used for authentication and encryption on the VAP interface.

Enter key values that match the key type and length settings. Select 64 Bit, 128 Bit, or 152 Bit key length. Note that the same size of encryption key must be supported on all wireless clients. (Default: 64 Bit)

- **64 Bit:** Enter keys as 5 alphanumeric characters or 10 hexadecimal digits.
- **128 Bit:** Enter keys as 13 alphanumeric characters or 26 hexadecimal digits.
- **152 Bit:** Enter keys as 16 alphanumeric characters or 32 hexadecimal digits.



*WEP 152 is not supported on the MVP-8400 Touch Panel.*



*Key index and type must match that configured on all clients.*

## Wireless VAP Settings - WPA / WPA2 Setting

Wi-Fi Protected Access (WPA) employs a combination of technologies to provide an enhanced security solution for wireless networks. The WPA Pre-shared Key (WPA-PSK) mode for small networks uses a common password phrase that must be manually distributed to all clients that want to connect to the network.

WPA2 is a further security enhancement that includes the now ratified IEEE 802.11i wireless security standard. Both WPA and WPA2 provide very robust security through the support of the Advanced Encryption Standard (AES) and Temporal Key Integrity Protocol (TKIP) encryption ciphers (FIG. 31).

The screenshot shows the 'Wireless VAP1 WPA / WPA2 Setting' page in the AMX web interface. The page has a blue header with the AMX logo and navigation tabs: Basic, Channel, WEP, and WPA / WPA2. The main content area is titled 'Wireless VAP1 WPA / WPA2 Setting' and contains a form with the following fields:

- WPA / WPA2 Status:** Radio buttons for 'Enable' and 'Disable' (selected).
- Authentication:** Radio buttons for 'WPA-PSK', 'WPA2-PSK', 'WPA-WPA2-PSK Mix Mode', 'WPA', 'WPA2', and 'WPA-WPA2 Mix Mode'.
- Key Cipher:** Radio buttons for 'Auto' (selected), 'AES', and 'TKIP'.
- WPA / WPA2-PSK key:** A text input field.

At the bottom right of the form are 'Save' and 'Cancel' buttons. Below the form is a navigation bar with icons for Info, System, VAP1, VAP2, Network, Time & Log, and update.

FIG. 31 Wireless VAP 1 Setting - WPA-PSK Wireless Security



*The computationally intensive operations of AES encryption requires hardware support on client devices. Before implementing AES in the network, be sure that wireless client hardware is AES or WPA2 compliant.*

The items on this page include:

- **WPA/WPA2 Status:** Enables WPA-PSK or WPA2-PSK security on the VAP interface. When enabled, WEP clients are not supported. (default: *Disabled*).
- **Authentication:** Select an authentication method. Supported methods include:
  - WPA-PSK, WPA2-PSK, WPA2-PSK Mix Mode



*If you select WPA(2)-PSK, you must provide a Key (see WPA-PSK Key below).*

- WPA, WPA2, WPA-WPA2 Mix Mode



*If you select WPA(2), you must configure the Radius server settings for WPA / WPA2 authentication (see the Network Settings - Radius Server Setting section on page 37).*

- **Key Cipher Mode:** Selects the encryption cipher to use for multicast and unicast data traffic:
  - **Auto:** Uses TKIP for the multicast cipher and TKIP or AES for the unicast cipher depending on the capability of associated clients.
  - **AES:** Uses AES keys for both multicast and unicast encryption.
  - **TKIP:** Uses TKIP keys for both multicast and unicast encryption.



- **WPA-PSK Key:** Enter a key as an easy-to-remember form of letters and numbers. The key must be from 8 to 63 characters, which can include spaces. All wireless clients must be configured with the same key to communicate with the VAP interface.

## Network Settings

The WAP250G supports DHCP client, DHCP server and Network Address Translation (NAT). Point-to-Point Protocol over Ethernet (PPPoE) is also supported for users that have an IP address assigned automatically from an Internet service provider (ISP) through an ADSL modem. Use the options on the Network Settings pages to configure the LAN and WAN network settings (FIG. 32).



FIG. 32 Network Settings - main page

### Network Settings - DHCP Client Setting

Configuring the WAP250G with an IP address enables you to manage the WAP250G from any PC in the attached network. A number of WAP250G features depend on IP addressing to operate.



NOTE

*You can connect to the web browser interface to access IP addressing only if the WAP250G already has an IP address that is reachable through your network.*

By default, the WAP250G is configured with the IP address **192.168.1.240**, with the DHCP client **disabled** (FIG. 33).

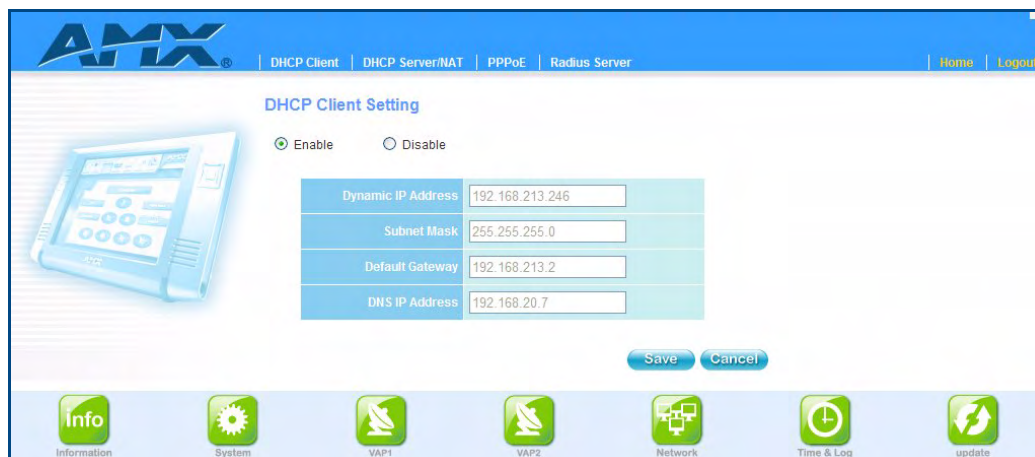


FIG. 33 Network Settings - DHCP Client Settings

The items on this page include:

- **DHCP Client Setting:** Enables the WAP250G to automatically obtain an IP address from a DHCP server. If a response is not received from the DHCP server, the WAP250G uses the fixed IP settings as configured on this page. When set to disabled, a static IP address can be manually configured.
- **Static IP Address:** The IP address of the WAP250G. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- **Subnet Mask:** The mask that identifies the host address bits used for routing to specific subnets.
- **Default Gateway:** The default gateway is the IP address of the router for the WAP250G, which is used if the requested destination address is not on the local subnet. If you have management stations located on another subnet, type the IP address of the default gateway router in the text field provided. Otherwise, leave the address as all zeros (0.0.0.0).
- **DNS IP Address:** The IP address of a Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

If you have a DNS server located on the local network, type the IP address in the text field provided. Otherwise, leave the address as all zeros (0.0.0.0).

### Network Settings - DHCP Server/NAT Setting

The WAP250G includes a Dynamic Host Configuration Protocol (DHCP) server that can assign temporary IP addresses to wireless clients requesting the service (FIG. 34).

**FIG. 34** Network Settings - DHCP Server/NAT Settings

Addresses are assigned to clients from a common address pool configured on the WAP250G. Configure an address pool by specifying start and end IP addresses. Be sure not to include the WAP250G's IP address in the address pool range.

Network Address Translation (NAT) is a standard method of mapping multiple "internal" IP addresses to one "external" IP address on devices at the edge of a network. For the WAP250G, the internal (local) IP addresses are the IP addresses assigned to wireless clients by the DHCP server, and the external IP address is the IP address assigned to the Ethernet port. When enabled, the WAP250G's wireless interface uses the NAT IP settings to access the Ethernet network.

When the DHCP server is enabled, NAT is also enabled.

The items on this page include:

- **DHCP Server/NAT Setting:** Enables or disables the DHCP server and NAT on the WAP250G. (Default: Enabled)
- **Start/End IP Address:** Specifies the start/end IP address of a range that the DHCP server can assign to DHCP clients. You can specify a single address or an address range.
- **Gateway:** The IP address of the gateway router for the WAP250G, which is used if the requested destination address is not on the local subnet.
- **DNS IP Address:** The IP address of a Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

### Network Settings - PPPoE Setting

Many Internet service providers (ISPs) use the Point-to-Point Protocol over Ethernet (PPPoE) to automatically assign an IP address to users with a DSL modem. The PPPoE page provides the settings needed for this service (FIG. 35).

**FIG. 35** Network Settings - PPPoE Settings

The items on this page include:

- **PPPoE Setting:** Enables the WAP250G IP address to be assigned automatically from an Internet service provider (ISP) through an ADSL modem using PPPoE.
- **Username:** If your ISP has provided you with a PPPoE user name, enter it in the corresponding text box.
- **Password:** If your ISP has provided you with a PPPoE password, enter it in the corresponding text box.



## Network Settings - Radius Server Setting

Radius (Remote Authentication Dial In User Service) is an authentication, authorization and accounting protocol for applications such as network access or IP mobility. It is intended to work in both local and roaming situations. Use the options on the *Radius Server Setting* page to configure Radius server settings for wireless clients (FIG. 36).

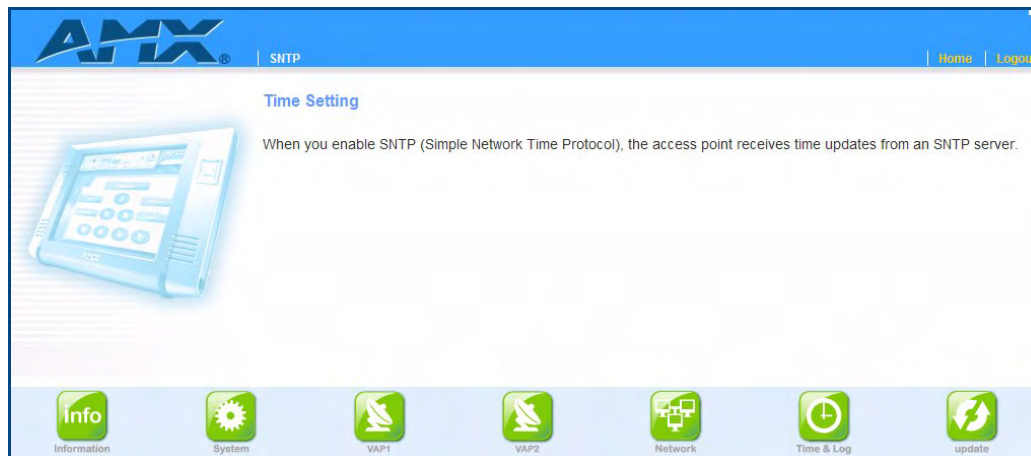
**FIG. 36** Network Settings - Radius Server Settings

The items on this page include:

- **Server Name / IP Address:** Enter the hostname or IP address of the Radius server that the WAP250G will connect to.
- **Port Number:** Enter the port number on the Radius server that will be used by the WAP250G.
- **New Secret Key:** Enter the Secret Key of the Radius Server, this secret key helps establishing the communication with the Radius server.
- **Confirm New Secret Key:** Re-enter the Secret Key.
- **Group Key Update Interval (secs):** Set the interval for Group Key Updates on the Radius server, in one-second increments (default = 1800, or 3 minutes).

## Time and Log

Use the options on the *Time Setting* page (FIG. 37) to enable Simple Network Time Protocol (SNTP). SNTP allows the WAP250G to set its internal clock based on periodic updates from a time server (SNTP or NTP).



**FIG. 37** Time Setting page

Maintaining an accurate time on the WAP250G enables all system log messages to be stamped with the correct time and date. If the clock is not set, the WAP250G only records the time from the factory default set at the last bootup.

The WAP250G acts as an SNTP client, which periodically sends time synchronization requests to a specific time server. SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display the time corresponding to your local time, you must also indicate the number of hours your time zone is located before or after UTC/GMT (FIG. 38).



**FIG. 38** Time Setting - SNTP Settings

The items on this page include:

- **SNTP Server Setting** — Configures the WAP250G to operate as an SNTP client. When enabled, the time server IP address must be specified.
- **Primary Server**: The IP address of an SNTP or NTP time server that the WAP250G attempts to poll for a time update.
- **Time Zone** — Sets the number of hours your local time zone is located before or after UTC/GMT. (Default: GMT+00)
- **Daylight Saving** — The WAP250G provides a way to automatically adjust the system clock for Daylight Savings Time changes. To use this feature you must define the month and date to begin and to end the change from standard time. During this period the system clock is set back by one hour.

## Updating Firmware

You can upgrade new WAP250G software from a local file on the management workstation, or from an FTP or TFTP server. Use the options on the *Firmware Upgrade* page to update the access point system software (FIG. 39).

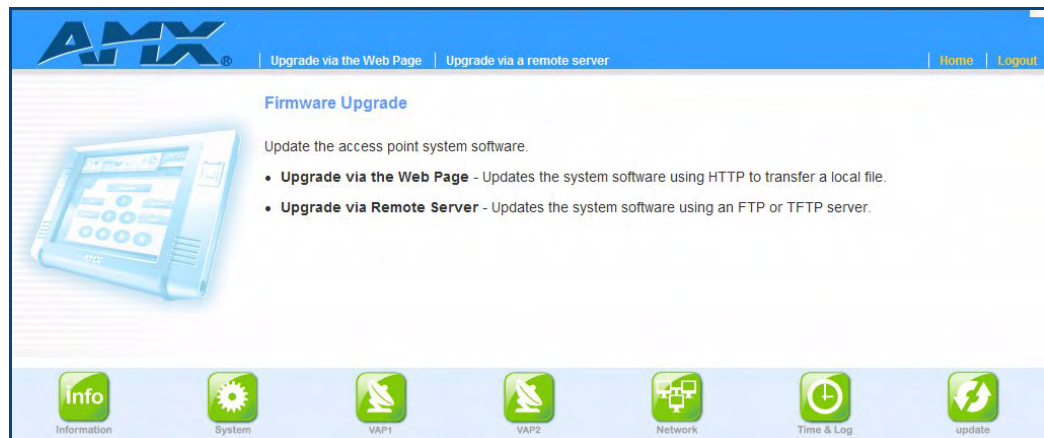


FIG. 39 Firmware Upgrade - main page

After upgrading to new software, you must reboot the WAP250G to implement the new code. Until a reboot occurs, the WAP250G will continue to run the software it was using before the upgrade started.

### Upgrade via the Web Page

The *Local File* page allows you to update the system software using HTTP to transfer a local file (FIG. 40).

The items on this page include:

- **New Firmware File** — Specifies the name of the code file on the local web management station. You can use the Browse button to locate the image file locally on the management station.
- **Start Upgrade** — Starts the download process. Be sure to allow enough time for the download to complete before rebooting the WAP250G.

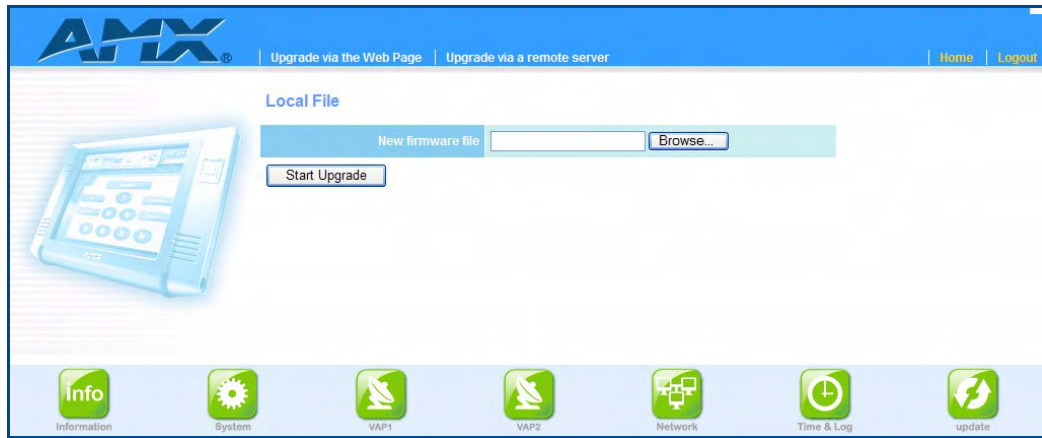


FIG. 40 Firmware Upgrade - Local File

### Upgrade via a Remote Server

The *Remote File* page allows you to download a new software code file from a remote server to the WAP250G using FTP or TFTP (FIG. 41).

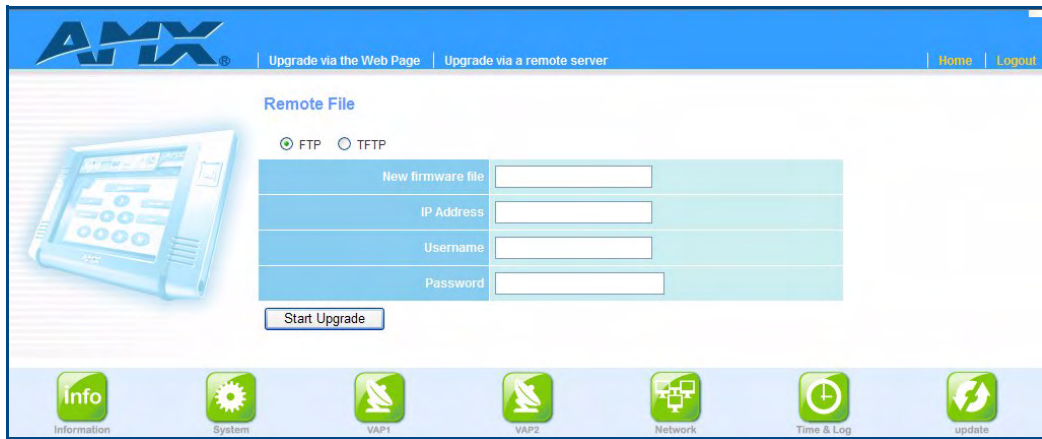


FIG. 41 Firmware Upgrade - Remote File

When using an FTP or TFTP server, be sure to first obtain the IP address of the server and note the correct file path where the WAP250G software is stored. If upgrading from an FTP server, also make sure that you have a user account configured on the server with a user name and password.

The items on this page include:

- **Remote File** — Specifies a software code file download from a remote FTP or TFTP server.
- **New firmware file** — Specifies the name of the code file on the server. A path on the server can be specified using “/” in the destination file name, providing the path already exists. Other than to indicate a path, the file name must not contain any slashes (\ or /), the leading letter cannot be a period (.), and the maximum length for file names on the FTP/TFTP server is 255 characters or 32 characters for files on the WAP250G. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “\_”)
- **IP Address** — IP address or host name of the FTP or TFTP server.
- **Username** — The user ID used for login to an FTP server.
- **Password** — The password used for login to an FTP server.

- **Start Upgrade** — Starts the download process. Be sure to allow enough time for the download to complete before rebooting the WAP250G.



*When you have downloaded the software file, you must reboot the WAP250G to implement the new code.*



# Appendix A: Troubleshooting

## Overview

Check the following items before you contact local Technical Support.

1. If wireless clients cannot access the network, check the following:
  - Be sure the NXA-WAP250G and the wireless clients are configured with the same Service Set ID (SSID).
  - If authentication or encryption are enabled, ensure that the wireless clients are properly configured with the appropriate authentication or encryption keys.
2. If the NXA-WAP250G cannot be configured using a web browser:
  - Be sure to have configured the NXA-WAP250G with a valid IP address, subnet mask and default gateway.
  - If you are connecting to the NXA-WAP250G through the wired Ethernet interface, check the network cabling between the management station and the NXA-WAP250G. If you are connecting to NXA-WAP250G from a wireless client, ensure that you have a valid connection to the NXA-WAP250G.
3. If you forgot or lost the password:
  - Set the NXA-WAP250G to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Connect to the web management interface using the default IP address 192.168.1.240. Then use the default user name “Admin” and the default password “1988” to access the management interface.
4. If all other recovery measure fail, and the NXA-WAP250G is still not functioning properly, take any of these steps:
  - Reset the NXA-WAP250G’s hardware using the web interface or through a power reset.
  - Reset the NXA-WAP250G to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Connect to the web management interface using the default IP address 192.168.1.240, then use the default user name “Admin” and the default password “1988.”

## If Your WAP250G Is Stuck on the Emergent Recovery Screen

### Step 1: Website for free TFTP Server

1. Connect to the internet and enter the following link in the Address Bar on your web browser.  
**<http://www.solarwinds.net/downloads/index.aspx>**
2. Scroll to the bottom of the page and click **Download Free TFTP Server** located at the bottom of the page (you will have to enter name, e-mail etc...).

### Step 2: Choose Download site and Install TFTP Server

1. Select any one of the three links that appear on the screen to begin download.
2. Click **Run** - to install software on your computer
3. Click **Run** again to begin the software install.
4. Select all of the defaults during the installation



### Step 3: Copy Firmware file

1. E-mail a copy of the firmware file ZZ-IMG.BIN (Firmware file 1.0.4.6) to the dealer.
2. Copy the file into the C:\TFTP-ROOT directory

### Step 4: Ethernet Connectivity

1. Verify the Ethernet port is enabled and connect an Ethernet cable from the laptop to the WAP250G.
2. Highlight **My Network Places**; Right-click **Properties**, Highlight **TCP/IP Settings** and click **Properties**.
3. Assign a static IP Address on the same network as the WAP250
4. Click **OK**.
5. Click **OK**.
6. Click **Start/Run** and type **CMD**.
7. **Ping** IP Address of the WAP250G to verify connectivity.

### Step 5: Launch TFTP Server

1. Start\Run\Program
2. Select **Solarwinds Free Tools**.
3. Select **TFTP Server** - the following window launches (FIG. 42):

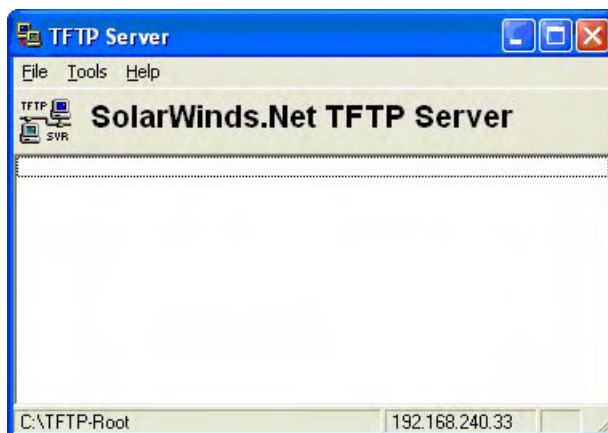
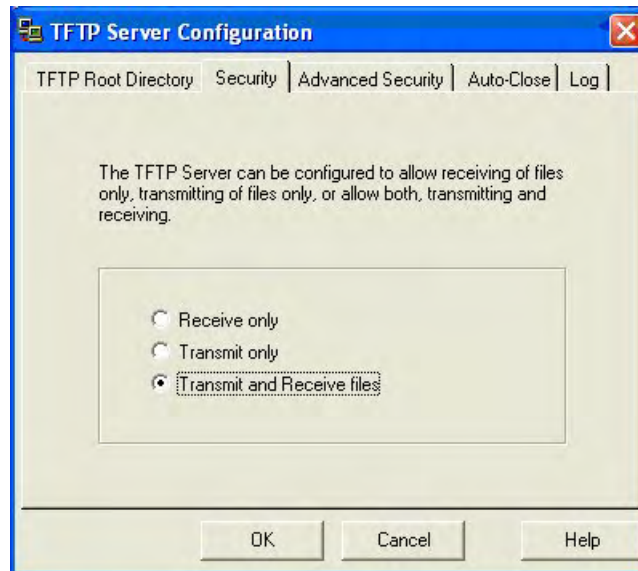


FIG. 42 SolarWinds.NET TFTP Server dialog

4. The IP Address should reflect the same IP Address of your Ethernet port on your laptop and the default directory (**C:\TFTP-Root**) is displayed on the bottom left.

### Step 6: Change TFTP Server Settings

1. Select **File**.
2. Select **Configure**.
3. Select the **Security Tab** and change selection to **Transmit and Receive Files** (FIG. 43).
4. Click **OK**.



**FIG. 43** TFTP Server Configuration dialog

### Step 7: Re-Connect to WAP 250G

1. Open a web browser and enter the IP Address for the WAP250G.
2. Follow the Emergent Recovery System on-screen prompts to begin the Firmware upload.







It's Your World - Take Control™

3000 RESEARCH DRIVE, RICHARDSON, TX 75082 USA • 800.222.0193 • 469.624.8000 • 469-624-7153 fax • 800.932.6993 technical support • [www.amx.com](http://www.amx.com)

5/07 ©2007 AMX. All rights reserved. AMX and the AMX logo are registered trademarks of AMX. AMX reserves the right to alter specifications without notice at any time.